NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF ARTS AND SOCIAL SCIENCES

COURSE CODE: CSS 442

COURSE TITLE:
Professional Ethics in Law Enforcement and Security Management

Course Guide

CSS 442
Professional Ethics in Law Enforcement and Security Management

Course Writers/Developers	Dr. R.A Okunola U.I Dr. Niyi Adegoke NOUN and Dr.A.D Ikuomola (Adekunle Ajasin University)
Course Editor	Dr. N.Nwabueze NOUN
Course Coordinators	Dr. Niyi Adegoke NOUN Mr. Igwe, D. O.NOUN Mr. C.A .C. Chukwunka NOUN
Programme Leader	Dr. N.Nwabueze NOUN

INTRODUCTION

CSS 442: Professional Ethics in Law Enforcement and Security Management is a 3-credit unit course. It is a compulsory course for both undergraduate and postgraduate students in the field of Criminology and Security Studies of the University. The course is also recommended to any other student(s) particularly those in the school of Arts and Social Sciences, who may have interest in the study and survey of Professional Ethics in Law Enforcement and Security Management. The course can also be taken as elective or required course by other Students whose main field(s) of discipline is not Criminology and Security Studies. However the course shall consist of 20 units, which include: police ethics: establishing the ethical climate, the importance of ethics in criminal justice, police ethics: a case study of turkey, natural law and ethical dilemmas, law enforcement code of ethics and the use of authority, law enforcement agencies and taser usage, intelligence agencies support and law enforcement, police accountability: evidence from united kingdom, internal strategies for building police-community trust, external strategies for building

community trust, internal affairs as an effective tool for building trust, security and ecology in the age of globalization, security and ecology in the age of globalization, information security: *e-government and denial of service (dos) attacks.* DDOS tools: a security threat, securing the computer systems, Africa and private security, contractors as military professionals in security management, community policing — working together to prevent crime, policing terrorism and threat to community policing are given special attention with the aim of stimulating effective knowledge of Professional Ethics in Law Enforcement and Security Management situations and agenda in the world so that students can identify, analyse, and proffer solutions to various aspect of conventional, modern and traditional safety management in the work place, at other civil arena and everyday living.

The course has no compulsory prerequisite for it to be registered for. The course guide informs us on what this course is all about, what students should appreciate in each unit, what text materials we shall be using and how we can make best use of these materials. This course guide also emphasises on the need for students to take tutored marked assignments so seriously. However, necessary information on tutored marked assignments shall be made known to students in a separate file, which will be sent to each of them at appropriate time. This course is also supported with periodic tutorial classes.

What You Will Learn In This Course

CSS 442 Professional Ethics in Law Enforcement and Security Management as a course in the field of Criminology and Security Studies at the National Open University of Nigeria focuses on a wide range of issues that bother on morals and expectations from law enforcement agents in carrying out their activities In this course we will carefully analyse ethics and ethical relativism and others such as the concepts of ethical Absolutism and pluralism emphasising the existence of an eternal and unchanging moral law, the same for all people, at all times and places vis-à-vis the Pluralists argument that in most situations there are many truths rather than one single truth about morality which should form the basis of life and decision making. Similarly other aspects professionalism regarding assess and usage of powers vested to law enforcement agents, police accountability and best practices in security operations with emphasis also on community policing, terrorism in a globalised world are discussed. Ethics alongside professionalism gives a broad perspective of human existence and diversity.

Course Aims

CSS 442 Professional Ethics in Law Enforcement and Security Management as a course is to introduce you to the concept of ethics, principles of oath of office and professionalism. It is also aimed at exposing student or reader to knowing most of the existing aspects of professionalism and changing ethics and professionalism in private and public security management. Undoubtedly, the way the course draws its references from the community and other related

happening in countries of Europe and America. The course is also aimed at understanding:

- Police ethics:
- Ethical climate,
- The importance of ethics in criminal justice
- Police ethics: a case study of turkey,
- Natural law and
- Ethical dilemmas,
- Law enforcement code of ethics
- The use of authority,
- Law enforcement agencies and taser usage,
- Intelligence agencies support and law enforcement
- Police accountability: evidence from united kingdom,
- Internal strategies for building police-community trust,
- External strategies for building community trust,
- Internal affairs as an effective tool for building trust,
- Security and ecology in the age of globalization,
- Information security: *e-government and denial of service (dos) attacks*. DDOS tools: a security threat,
- Securing the computer systems,
- Africa and private security,
- Contractors as military professionals in security management,
- Community policing
- Policing terrorism and threat to community policing

Course Objectives

With utmost desire to achieve the aims set out above, the course has some set of objectives as demonstrated in all the units of the course. Each unit has its own objectives. Objectives are always included at the beginning of every unit to assist the student in appreciation of what he or she will come across in the study of each unit to facilitate his or her better understanding of the course CSS 442: Professional Ethics in Law Enforcement and Security Management. Students are therefore advised to read these objectives before studying the entire unit(s). Thus, it is helpful to do so. You should always look at the unit objectives after completing a unit. In this way, you can be sure that you have done what was required of you by the unit. Stated below are the wider objectives of this course as a whole. By meeting these objectives, you should have achieved the aims of the course as a whole.

At the end of the course, you should be able to:

- Define and explain the concept of ethics,
- Highlights the importance of ethics in any profession,
- Understand ethical climate in the workplace,

- Differentiate ethics and natural laws,
- Explain, the dilemmas of ethics,
- Examine the use of authority,
- Discuss law enforcement code of ethics,
- Explain police accountability,
- Examine intelligence agencies support and law enforcement,
- Examine internal and external strategies for building police-community trust,
- Discuss internal affairs as an effective tool for building trust,
- Examine security and ecology in the age of globalization,
- Discuss the concept of e-security and e-government,
- Discuss the proliferation of private security in Africa,
- Examine community policing and the policing of terrorism,
- Lastly to explain the relevance of military professionals in security management.

Working through this course

In completing this course, students are required to study the whole units, and try to read all (or substantial number of) the recommended textbooks, journals and other reading materials including electronic resources. Each unit contains self assessment exercise(s) and students are required to submit their assignments for the purpose of assessment. At the end of the course, student(s) shall be examined. The time of the final examination and venue shall be communicated to all the registered students in due course by relevant school authorities-study centre management. Below are the components of the course and what you are required to do:

Course Materials

Major component of the course include:

1. Course Guide
2. Study Units
3. Textbooks
4. Assignments Files
5. Presentations Schedule

It is incumbent upon every student to get his or her own copy of the course material. You are also advised to contact your tutorial facilitator, if you have any difficulty in getting any of the text materials recommended for your further reading.

Study Units

In this course there are twenty units, divided into four modules, (five in each module). Below are the units:

Module 1
Unit 1. Police Ethics: Establishing the Ethical Climate
Unit 2. The Importance of Ethics in Criminal Justice
Unit 3. Police Ethics: A Case Study of Turkey
Unit 4. Natural Law and Ethical Dilemmas
Unit 5. Law Enforcement Code of Ethics and the Use of Authority

Module 2
Unit 1. Law Enforcement Agencies and Taser Usage
Unit 2. Intelligence Agencies Support and Law Enforcement
Unit 3. Police Accountability: Evidence from United Kingdom
Unit 4. Internal Strategies for building Police-Community Trust
Unit 5. External Strategies for Building Community Trust

Module 3
Unit 1. Internal Affairs as an Effective Tool for Building Trust
Unit 2. Security and ecology in the age of globalization
Unit 3. Security and ecology in the age of globalization ii
Unit 4. Information security: *E-government and Denial of Service (DoS) Attacks.*
Unit 5. DDoS Tools: A Security Threat

Module 4
Unit 1. Securing the Computer Systems
Unit 2. Africa and Private Security
Unit3. Contractors as Military Professionals in Security Management
Unit 4. Community Policing — Working Together to Prevent Crime
Unit 5. Policing Terrorism: A Threat to Community Policing

Text books, Journals and References

Course Material

The following Text books, Journals are course material recommended to each student taking the course.

Required Readings:

Kane, R. 1996. *Through the Moral Maze: Searching for Absolute Values in a Pluralistic World.* Armonk, NY: North Castle Books.

Ladd, John. 1973. *Ethical Relativism.* Belmont, CA: Wadsworth. “92nd death row inmate freed since ’73: Louisiana.” January 5, 2001. *New York.*

Lynch, G. W. (1999) *Human Dignity and the Police: Ethics and Integrity in Police Work*, Illinois: Charles C Thomas.

Arrington, R. 1983. "A Defence of Ethical Relativism." *Metaphilosophy* 14: 225–239.

Bunting, Harry. 1996. "A Single True Morality? The Challenge of Relativism." Pp. 73–85 in *Philosophy and Pluralism*, edited by David Archard. Cambridge: Cambridge University Press.

Brace. Holmes, Robert. 1998. *Basic Moral Philosophy* (4th ed.). Belmont, CA: Wadsworth.

Bryden, A. and Fluri, H. P. (Eds) (2003) *Security Sector Reform: Institutions, Society and Good Governance*, Baden-Baden: Nomos Verlagsgesellschaft.

Felkenes, G. 1987. "Ethics in the Graduate Criminal Justice Curriculum." *Teaching Philosophy* 10(1): 23–26.

Glover, Jonathan. 1999. "Capital Punishment." Pp. 245–253 in *The Right Thing to Do: Basic Readings in Moral Philosophy* (2nd ed.), edited by J. Rachels. Boston: McGraw-Hill.

Hackman, M. J. *Citizen Complaints About Police Use of Force: Bureau Justice of Statistics*

Hanggi, H. Winkler, T. H. (2003) *Challenges of Security Sector Governance*, Geneva Center for the Democratic Control of Armed Forces.

Hare, R. M. 1987. "Moral Conflicts." Pp. 205–238 in *Moral Dilemmas*, edited by C. Gowans. New York: Oxford University Press.

Hinman, L. 1998. *Ethics: A Pluralistic Approach to Moral Theory*. Fort Worth, TX: Harcourt

ACLU of Northern California, "Stun Gun Fallacy: How the Lack of Taser Regulation Endangers Lives," September 2005 ("ACLU Report"), p. 4, citing Russel Sabin, "Heart Expert Warns About Using Tasers," San Francisco Chronicle, January 5, 2005.

Alexandria, Virginia: International Association of Chiefs of Police, 2002. www.theiacp.org/LinkClick.aspx?fileticket=4B%2f4SDZtgV8%3d&tabid=392

http://www.caida.org/outreach/papers/2003/sapphire/index.xml (last modified Sept. 11, 2003) Association of Chiefs of Police, National Law Enforcement Policy Center, Alexandria,

Bureau of National Affairs (2002). Berman to Introduce Bill Aimed at Curbing Piracy over Internet Peer-To-Peer Networks, 64 PAT. Trademark & Copyright J. 190

Cook, John. 1999. *Morality and Cultural Differences.* New York: Oxford University Press.

Death Watch. 2002. "New Orleans: Recent History 1996." Retrieved January 28, 2002 (www. hrw.org/reports98/police/uspo93.htm).

http://www.amnestyusa.org/countries/usa/document.do?id=1A01E91E134A327080256F190042408D. Amnesty International, "Excessive and Lethal Force? Amnesty International's Concerns

http://www.amnestyusa.org/countries/usa/document.do?id=1A01E91E134A327080256F190042408D

http://www.cpoa.org/forcechart.html for a visual representation of the use of force continuum
http://www.taser.com/law/download/memo.htm. (Taser Memo).

IACP Report. http://www.iacp.org/research/CuttingEdge/EMDT9Steps.pdf.

Jay Lyman, When the Haked Becomes the Haker, Nov. 19, 2001, at http://www.newsfactor.com/perl/story/14874.html/ (on file with the Yale Journal of Law & Technology).

Jean Braucher, Uniform Computer Information Transactions Act (UCITA): Objections Justice Programs, National Institute of Justice. *Police Integrity – Public Service with Honor,*

Maj. David DiCenso, The Legal Issues of Information Warfare, 13 AIRPOWER J. 85, 95 n.66 (1999), available at http://www.airpower.maxwell.af.mil/ airchronicles/apj/apj99/sum99/dicenso.

Munteanu, T. (2005) 'Reforming the security sector: The experience of the SEE and the Black Sea region', paper presented to the Halki International Seminars 2005 – on *Security Sector Reform in South Eastern Europe and the Mediterranean: Lessons and Challenges*, 7-11 September 2005, Greece.

Policing Services. Washington, D.C., January 1997. www.ncjrs.gov/pdffiles/163811.pdf

Qatarneh, Y. (2005) 'Civil-military realations and security sector reform in the Arab world', paper presented to Halki International Seminars 2005- *on Security*

Sector Reform in South Eastern Europe and the Mediterranean: Lessons and Challenges, 7-11 September 2005, Greece.

Rachels, J. 1991. "Subjectivism." Pp. 432–441 in *A Companion to Ethics*, edited by P.

Reiter, L. *Law Enforcement Administrative Investigations: A Supervisory and Agency Guide*

Robert L. Mitchell, Reality Intrudes On the Internet, COMPUTERWORLD at 44, Sept. 3, 2001.

Services and International City/County Management Association, 2007.

Singer, Peter. 1995. *How Are We to Live? Ethics in an Age of Self-Interest.* Amherst, NY: Prometheus Books. Singers. Cambridge, MA: Blackwell Press.

Special Report. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, Taser International website, Product Warnings for Law Enforcement. www.taser.com/safety.

Thurnauer, B. (2002) *Best Practice Guide, Internal Affairs: A Strategy for Smaller Departments*. *Times*. Retrieved January 2002 (www.truthinjustice. org/no92.htm).
to: Handle Citizen Complaints of Misconduct, Conduct Administrative Investigations, Manage the Internal Affairs Function, and Create Reasonable and Defensible Discipline 2nd Edition. Tallahassee, Florida: Lou Reiter and Associates, 2004.

U.S. Department of Justice, Office of Community Oriented Policing Services and Office of Uniform Computer Information Transactions Act (UCITA), 2002, available at http://www.law.upenn.edu/bll/ulc/ulc_frame.htm. Virginia: 2007.

Winn Schwartau, Cyber-Vigilante Hunt Down Hackers, CNN.COM, Jan. 12, 1999, at www.cnn.com/TECH/computing/ 9901/12/cybervigilantes.idg/; see also Tedeschi supra note 4.

Womack, Mari. 1995. "Studying Up and the Issue of Cultural Relativism." *NAPA Bulletin* 16: 48. www.cops.usdoj.gov/files/RIC/Publications/cp_explained.pdf

Assignment File

In this file you will find the necessary details of the assignments you must submit to your tutor for assessment. The marks you get from these assignments will form part of your final assessment in this course,

Assessment

There are two aspects to the assessment of the course. First are the tutor-marked assignment; second there is the written examination. In tackling the assignments, you are expected to apply information and knowledge acquired during this course. The assignments must be submitted to your tutor for assessment in accordance with the deadlines stated in the Assignment file. The work you submit to your tutor for assessment will count for 30% of your total course work. At the end of the course, you will need to sit for a final three-hour examination. This will also count for 70% of your total course mark.

Tutor- Marked Assignment

There are twenty tutor-marked assignments in this course. You need to submit four assignments out of which the best three will be used for your assessment. These three assignments shall make 30% of your total course work. Assignment question for the units in this course are contained in the assignment file. You should be able to complete your assignments from the information and materials contained in your set textbooks, reading and study units. However, you are advised to use other references to broaden your view point and provide a deeper understanding of the subject. When you have completed each assignment, send it together with TMA (Tutored-Marked Assignment) file to your tutor. Make sure that each assignment gets to your tutor on or before the deadline. And in case of being unable to complete your work on time, contact your tutor or better still your study centre manager (overseer) before the submission deadline of assignments elapses to discuss the possibility of an extension**.**

Final examination and grading

The final examination of CSS 442 shall be of three hours duration and have a value of 70% of the total course grade. The examination shall consist of questions which reflect the type of self-testing. Practice exercises and tutor-marked problems you have come across. All areas of the course will be assessed. You are advised to revise the entire course after studying the last unit before you sit for the examination. You will find it useful to review your tutored-marked assignments and the comments of your tutor on them before the final examination.

Course Marking Scheme

This table shows how the actual course marking is broken down.

Assessment	Marks
Assignment 1-4	Four assignments are to be submitted, out of which the three best shall be considered at 10% each, making 30% of the overall scores
Final Examination	70% of overall course marks
Total	100% of course marks.

Table 1: Course Marking Scheme

Course Overview

The table brings together the entire units contained in this course, the number of weeks you should take to complete them, and the assignments that follow them.

Unit	Title	Week's Activity	Assessment (end of unit)
	Course Guide		
1.	Police Ethics: Establishing the Ethical Climate	1	Assignment 1
2.	The Importance of Ethics in Criminal Justice	2	Assignment 2
3.	Police Ethics: A Case Study	2	Assignment 3
4.	Natural Law and Ethical Dilemmas	3	Assignment 4
5.	Law Enforcement Code of Ethics and the Use of Authority	4	Assignment 5
6.	Law Enforcement Agencies and Taser Usage	5	Assignment 6
7.	Intelligence Agencies Support and Law Enforcement	6	Assignment 7
8.	Police Accountability: Evidence from United Kingdom	6	Assignment 8
9.	Internal Strategies for building Police-Community Trust	7	Assignment 9
10.	External Strategies for Building Community Trust	7	Assignment 10
11.	Internal Affairs as an Effective Tool for Building Trust	8	Assignment 11
12.	Security and ecology in the age of globalization	9	Assignment 12
13.	Security and ecology in the age of globalization ii	10	Assignment 13
14.	Information security: E-government and Denial of Service (DoS) Attacks.	11	Assignment 14
15.	DDoS Tools: A Security Threat	11	Assignment 15
16.	Securing the Computer Systems	12	Assignment 16
17.	Africa and Private Security	13	Assignment 17

18.	Contractors as Military Professionals in Security Management	14	Assignment 18
19.	Community Policing — Working Together to Prevent Crime	15	Assignment 19
20.	Policing Terrorism: A Threat to Community Policing	16	Assignment 20
21.	Revision	17	
22.	Examination	18	

Table 2: Course Overview

Presentation Schedule

The presentation Schedule included in your course materials gives you the important dates for the completion of tutor-marked assignments and attending tutorials. Remember you are required to submit all your assignments by the due date. You should guard against falling behind in your work.

How To Get The Best From This Course

In distance learning the study units replace the university lecturer. This is one of the great advantages of distance learning; you can read and work through specially designed study materials at your own pace, and at a time and place that suit you best. Think of it as reading the lecture instead of listening to a lecturer. In this same way that a lecturer might set you some reading to do, the study units tell you when to read your set of books or other materials. Just as a lecturer might give you an in-class exercise, your study units provide exercises for you to do at appropriate points. Each of the study units follows a common format. The first item is an introduction to the subject matter of the unit and the course as a whole. Next is a set of learning objectives. These objectives shall let you know what you should be able to do by the time you have completed the unit. You should use these objectives to guide your study. When you have finished the units, you must go back and check whether you have accepted the objectives. If you have a habit of doing this you will significantly improve your chances of passing the course. The main body of the unit guides you through the required reading from other sources.

Reading Section

Remember that your tutor's job is to assist you. Whenever you need help, do not hesitate to call and ask your tutor to provide it.

1. Read this Course Guide thoroughly.

2. Organised a Study Schedule. Refer to the 'Course Overview' for more details. Note the time you are expected to spend on each unit and how the assignments related to the units. Whatever method you chose to use, you should decide on and write in your own dates for working on each unit.

3. Once you have created your own study schedule, do everything you can to stick to it. The major reason why students fail is that they get behind with their course work. If you get into difficulties with your schedule, please let your tutor know it is too late for help.

4. Turn to unit 1 and read the introduction and the objectives for the unit.

5. Assemble the study materials. Information about what you need for a unit is given in the 'Overview' at the beginning of each unit. You will almost

always need both the study unit you are working on and one of your set books on your desk at the same time.

6. Work through the unit. The content of the unit itself has been arranged to provide a sequence for you to follow. As you work through the unit s you will be instructed to read sections from your set books or other materials. Use the unit to guide your reading.

7. Review the objectives for each study unit to confirm that you have achieved them. if you feel unsure about any of the objectives, review the study materials or consult your tutor.

8. When you are confident that you have achieved a unit's objectives, you can then start on the next unit. Proceed unit by unit through the course and try to pace your study so that you keep yourself on schedule.

9. When you have submitted an assignment to your tutor for marking, do not wait for its return before starting on the next unit. Keep to your schedule. When the assignment is returned pay particular attention to your tutor's comments, both on the tutor-Marked Assignment from and also on what is written on the assignment. Consult your tutor as soon as possible if you have any questions or problems.

10. After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unit) and the course objectives (listed in this Course-Guide).

Facilitators/Tutors and Tutorials

There are between eight (8) and twelve (12) hours of tutorials provided in support of this course. The dates, time and venue of these tutorials shall be communicated to you. The name and phone number of your tutor will be made available to you immediately you are allocated a tutorial group. Your tutor will mark and comment on your assignments, keep a close watch on your progress and on any difficulties you might encounter and provide assistance to you during the course. You must mail your tutor marked assignments to your tutor well before the due date (at least two working days are required). They will be marked by your tutor and returned to you as soon as possible. Do not hesitate to contact your tutor by phone, e-mail, or discussion board if you need help. You will definitely benefit a lot by doing that. Contact your tutor if:

- You do not understand any part of the study units or the assigned readings;
- You have difficulty with the self-tests or exercises; and ;

- You have a question or problem with an assignment, with your tutor's comment on an assignment or with the grading of an assignment.

You should make an effort to attend the tutorials. Thus, it is the only opportunity you have to enjoy face contact with your tutor and to ask questions which are answered instantly. You can raise any problem encountered in the course of your study. To gain the maximum benefits from the course tutorials, prepare a question list before attending them. You will learn a lot from participating in discussion actively.

Summary

- CSS: 342 aims to expose you to issues, ideas and methodologies, framework in engaging some common technicalities in Safety Management for Loss Prevention as well as policies as internationally demanded in safeguarding human life. As you complete this course, you should be able to answer and discuss reasonably the following:
  - The concept of safety ,
  - Issues in Safety Culture:
  - Key Health Issues,
  - Concept of Risk,
  - Safety and the Human Factor,
  - The basics of safety management and risk management,
  - Safety and Security in Nigeria :
  - Some Indicators of Violence,
  - Safety management in relation to building maintenance in Nigeria,
  - Public space and private security in the 21st century
  - Safety Measures on Construction Companies
  - Urban Crime Prevention Strategies in Africa,
  - Political, Religious and Ethnic Conflict In Nigeria**.**
  - The relevance of conflict management in safety management

Finally, you are advised to read the course material appreciably well in order to prepare fully and not to be caught pants down by the final examination questions. So, we sincerely wish you success in your academic career as you will find this course, CSS 442 very interesting. You should always avoid examination malpractices!

UNIT 1
Police Ethics: Establishing the Ethical Climate

1.0 Introduction

Being a chief of police entails "the process of influencing human behaviour to achieve organizational goals that serve the public, while developing individuals, teams, and the organization for future service." This leadership process is comprised of two component parts, direct and indirect leadership. One of the responsibilities of indirect leadership on the part of a chief of police is to influence the members of the department through shaping the context for ethical behaviour in the delivery of police services. As senior leaders, police chiefs set the context for ethical behaviour by the following:

1. Selecting people of good character to lead,
2. Setting an example of ethical behaviour at all times, avoiding even the perception of questionable actions or words,
3. Establishing clear guidelines for ethical behaviour and supportive norms,
4. Building support for sound values in all members of the department,
5. Developing the moral sensitivity and judgment of others,
6. Keeping competition and stress within functional limits,
7. Using rewards for ethical behaviour and punishments for unethical behaviour, and
8. Neutralizing forces in the department's working environment that could undermine ethical behaviour.

In the delivery of police services the authority to take a human life and to take away a person's freedom while maintaining his or her constitutional rights is delegated to the lowest level in the organization. To this end, in order to mitigate the effects of forces inside and outside the police department that

might diminish the character of the organization and its members in the ethical delivery of police services, the International Association of Chiefs of Police (IACP) offers the following four documents as foundational principles for establishing clear ethical guidelines within a police department.

• Law Enforcement Oath of Honor

• Law Enforcement Code of Ethics

• Law Enforcement Code of Conduct

• Canons of Police Ethics

2.0 Objectives

This unit examines some of the ethical principles guiding the police and their mode of operations. Students are therefore expected to know the four ethical principles vis avis ethical behaviours of law enforcement agents

3.0 Main body

IACP Ethics Toolkit

Enhancing Law Enforcement Ethics in a Community Policing Environment

The International Association of Chiefs of Police (IACP) and the U.S. Department of Justice Office of Community Oriented Policing Services (COPS Office) have created an Ethics Toolkit: Enhancing Law Enforcement Ethics in a Community Policing Environment.

"Ethics remains our greatest training and leadership need today."

Both the IACP membership and the COPS Office agree with the Police Image and Ethics Committee's finding and consider ethics an important training and leadership need. The toolkit they created is both a call to action and a resource guide to assist local law enforcement agencies. Local agencies using the activities and programs contained in this toolkit will heighten the awareness and visibility of law enforcement's ethical standards both internally and externally. The tools are to engage your agency in the building blocks of high ethical standards and to demonstrate your department's commitment to ethics and professionalism to your community.

The contents of this toolkit can be found on the IACP website at www.theiacp.org --Professional Assistance – Ethics. Below is a listing of the toolkits resources.

What is the Law Enforcement Oath of Honor?

An explanation of the elements, the resolution establishing the Law Enforcement Oath of Honor, and ways in which to present the oath.

Oath of Honor Video

Included in this toolkit is a video that reviews the Oath of Honor and its meaning.

Oath of Honor
A copy suitable for framing and displaying in your organization is included in this toolkit.

Sign-on Campaign
It is important that not only is the oath distributed and incorporated into ceremonies but that individual officers publicly record their commitments to high ethical standards.

Focus on Ethics: The Law Enforcement Oath of Honor
Statement by the IACP Police Image and Ethics Committee

Regional Community Policing Institutes
Established by the Office of Community Oriented Police Services, U.S. Department of Justice. Provides free ethics and integrity training courses.

Bibliography
This bibliography is of pertinent ethics and integrity literature produced in the law enforcement literature since 1990. This listing of resources will be useful for law enforcement training organizations, command staff and others interested in an in-depth review of the topic.

Reports/Resources
Specific reports and resources that focus on the issues of ethics and integrity

Model Policy on Standards of Conduct
This policy, developed by the IACP Policy Center, is provided for agencies to state with specificity the standards of conduct embodied in ethical conduct. Agencies can adopt or modify to meet their needs.

IACP In-service Training Material
Police Ethics: Problems and Solutions. This two-part Training Key, designed for in-service training of police officers, examines the nature and importance of police ethics and discusses some of the factors that affect police integrity in today's world. Specific suggestions that may help law enforcement agencies resolve some of the problems are identified.

The Public Image of the Police
Final report presented to the International Association of Chiefs of Police by the Administration of Justice Program, George Mason University reviewing the existing knowledge of the public image of the police up to the year 2000.

Law Enforcement

Oath of Honor
On my honor, I will never
betray my badge, my integrity,
my character or the public trust.
I will always have the courage to hold
myself and others accountable for our actions.
I will always uphold the constitution,
my community and the agency I serve..... International Association of Chiefs of Police

IACP Law Enforcement Code of Ethics
As a law enforcement officer, my fundamental duty is to serve the community; to safeguard lives and property; to protect the innocent against deception, the weak against oppression or intimidation and the peaceful against violence or disorder; and to respect the constitutional rights of all to liberty, equality and justice.

I will keep my private life unsullied as an example to all and will behave in a manner that does not bring discredit to me or to my agency. I will maintain courageous calm in the face of danger, scorn or ridicule; develop self-restraint; and be constantly mindful of the welfare of others. Honest in thought and deed both in my personal and official life. I will be exemplary in obeying the law and the regulations of my department. Whatever I see or hear of a confidential nature or that is confided to me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.

I will never act officiously or permit personal feelings, prejudices, political beliefs, aspirations, animosities or friendships to influence my decisions. With no compromise for crime and with relentless prosecution of criminals, I will enforce the law courteously and appropriately without fear or favor, malice or ill will, never employing unnecessary force or violence and never accepting gratuities.

I recognize the badge of my office as a symbol of public faith, and I accept it as a public trust to be held so long as I am true to the ethics of police service. I will never engage in acts of corruption or bribery, nor will Icondone such acts by other police officers. I will cooperate with all legally authorized agencies and their representatives in the pursuit of justice.

I know that I alone am responsible for my own standard of professional performance and will take every reasonable opportunity to enhance and improve my level of knowledge and competence.

I will constantly strive to achieve these objectives and ideals, dedicating myself before God to my chosen profession . . . law enforcement.

Law Enforcement Code of Conduct

The International Association of Chiefs of Police

All law enforcement officers must be fully aware of the ethical responsibilities of their position and must strive constantly to live up to the highest possible standards of professional policing. The International Association of Chiefs of Police believes it important that police officers have clear advice and counsel available to assist them in performing their duties consistent with these standards, and has adopted the following ethical mandates as guidelines to meet these ends.

Primary Responsibilities of a Police Officer

A police officer acts as an official representative of government who is required and trusted to work within the law. The officer's powers and duties are conferred by statute. The fundamental duties of a police officer include serving the community, safeguarding lives and property, protecting the innocent, keeping the peace and ensuring the rights of all to liberty, equality and justice.

Performance of the Duties of a Police Officer

A police officer shall perform all duties impartially, without favor or affection or ill will and without regard to status, sex, race, religion, political belief or aspiration. All citizens will be treated equally with courtesy, consideration and dignity. Officers will never allow personal feelings, animosities or friendships to influence official conduct. Laws will be enforced appropriately and courteously and, in carrying out their responsibilities, officers will strive to obtain maximum cooperation from the public. They will conduct themselves in appearance and deportment in such a manner as to inspire confidence and respect for the position of public trust they hold.

Discretion

A police officer will use responsibly the discretion vested in his position and exercise it within the law. The principle of reasonableness will guide the officer's determinations, and the officer will consider all surrounding circumstances in determining whether any legal action shall be taken. Consistent and wise use of discretion, based on professional policing competence, will do much to preserve good relationships and retain the confidence of the public. There can be difficulty in choosing between conflicting courses of action. It is important to remember that a timely word of advice rather than arrest— which may be correct in appropriate circumstances—can be a more effective means of achieving a desired end.

Use of Force

A police officer will never employ unnecessary force or violence and will use only such force in the discharge of duty as is reasonable in all circumstances.

The use of force should be used only with the greatest restraint and only after discussion, negotiation and persuasion have been found to be inappropriate or ineffective. While the use of force is occasionally unavoidable, every police officer will refrain from unnecessary infliction of pain or suffering and will never engage in cruel, degrading or inhuman treatment of any person.

Confidentiality
Whatever a police officer sees, hears or learns of that is of a confidential nature will be kept secret unless the performance of duty or legal provision requires otherwise. Members of the public have a right to security and privacy, and information obtained about them must not be improperly divulged.

Integrity
A police officer will not engage in acts of corruption or bribery, nor will an officer condone such acts by other police officers. The public demands that the integrity of police officers be above reproach. Police officers must, therefore, avoid any conduct that might compromise integrity and thus undercut the public confidence in a law enforcement agency. Officers will refuse to accept any gifts, presents, subscriptions, favors, gratuities or promises that could be interpreted as seeking to cause the officer to refrain from performing official responsibilities honestly and within the law. Police officers must not receive private or special advantage from their official status. Respect from the public cannot be bought; it can only be earned and cultivated.

Cooperation with Other Police Officers and Agencies
Police officers will cooperate with all legally authorized agencies and their representatives in the pursuit of justice. An officer or agency may be one among many organizations that may provide law enforcement services to a jurisdiction. It is imperative that a police officer assists colleagues fully and completely with respect and consideration at all times.

Personal-Professional Capabilities
Police officers will be responsible for their own standard of professional performance and will take every reasonable opportunity to enhance and improve their level of knowledge and competence. Through study and experience, a police officer can acquire the high level of knowledge and competence that is essential for the efficient and effective performance of duty. The acquisition of knowledge is a neverending process of personal and professional development that should be pursued constantly.

Private Life
Police officers will behave in a manner that does not bring discredit to their agencies or themselves. A police officer’s character and conduct while off duty must always be exemplary, thus maintaining a position of respect in the community in which he or she lives and serves. The officer’s personal behavior must be beyond reproach.

Canons of Police Ethics

Article 1. Primary Responsibility of Job

The primary responsibility of the police service, and of the individual officer, is the protection of the people of the United States through the upholding of their laws; chief among these is the Constitution of the United States and its amendments. The law enforcement officer always represents the whole of the community and its legally expressed will and is never the arm of any political party or clique.

Article 2. Limitations of Authority

The first duty of a law enforcement officer, as upholder of the law, is to know its bounds upon him in enforcing it. Because he represents the legal will of the community, be it local, state or federal, he must be aware of the limitations and proscriptions which the people, through law, have placed upon him. He must recognize the genius of the American system of government that gives to no man, groups of men, or institution, absolute power, and he must ensure that he, as a prime defender of that system, does not pervert its character.

Article 3. Duty to Be Familiar with the Law and with Responsibilities of Self and other Public Officials

The law enforcement officer shall assiduously apply himself to the study of the principles of the laws which he is sworn to uphold. He will make certain of his responsibilities in the particulars of their enforcement, seeking aid from his superiors in matters of technicality or principle when these are not clear to him; he will make special effort to fully understand his relationship to other public officials, including other law enforcement agencies, particularly on matters of jurisdiction, both geographically and substantively.

Article 4. Utilization of Proper Means to Gain Proper Ends

The law enforcement officer shall be mindful of his responsibility to pay strict heed to the selection of means in discharging the duties of his office. Violations of law or disregard for public safety and property on the part of an officer are intrinsically wrong; they are self-defeating in that they instill in the public mind a like disposition. The employment of illegal means, no matter how worthy the end, is certain to encourage disrespect for the law and its officers. If the law is to be honored, it must first be honored by those who enforce it.

Article 5. Cooperation with Public Officials in the Discharge of Their Authorized Duties

The law enforcement officer shall cooperate fully with other public officials in the discharge of authorized duties, regardless of party affiliation or personal prejudice. He shall be meticulous, however, in assuring himself of the propriety, under the law, of such actions and shall guard against the use of his office or person, whether knowingly or unknowingly, in any improper or illegal

action. In any situation open to question, he shall seek authority from his superior officer, giving him a full report of the proposed service or action.

Article 6. Private Conduct
The law enforcement officer shall be mindful of his special identification by the public as an upholder of the law. Laxity of conduct or manner in private life, expressing either disrespect for the law or seeking to gain special privilege, cannot but reflect upon the police officer and the police service. The community and the service require that the law enforcement officer lead the life of a decent and honorable man. Following the career of a policeman gives no man special perquisites. It does give the satisfaction and pride of following and furthering an unbroken tradition of safeguarding the American republic. The officer who reflects upon this tradition will not degrade it. Rather, he will so conduct his private life that the public will regard him as an example of stability, fidelity, and morality.

Article 7. Conduct toward the Public
The law enforcement officer, mindful of his responsibility to the whole community, shall deal with individuals of the community in a manner calculated to instill respect for its laws and its police service. The law enforcement officer shall conduct his official life in a manner such as will inspire confidence and trust. Thus, he will be neither overbearing nor subservient, as no individual citizen has an obligation to stand in neither awe of him nor a right to command him. The officer will give service where he can, and require compliance with the law. He will do neither from personal preference or prejudice but rather as a duly appointed officer of the law discharging his sworn obligation.

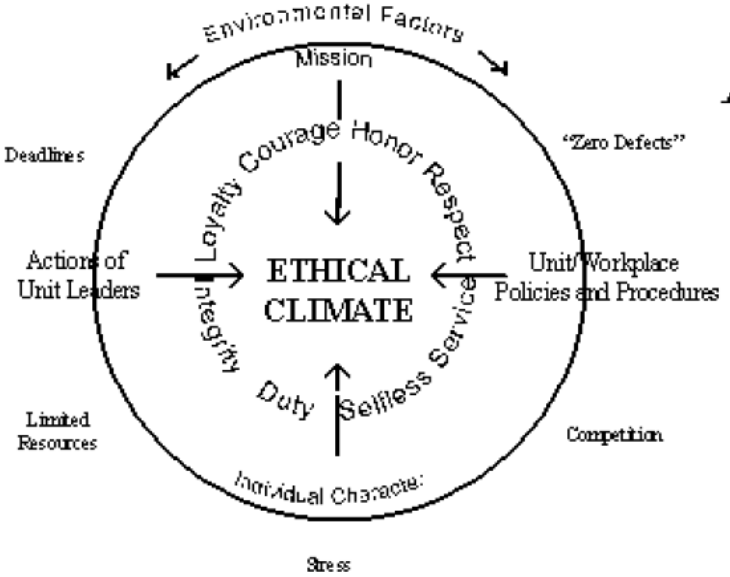
Article 8. Conduct in Arresting and Dealing with Law Violators
The law enforcement officer shall use his powers of arrest strictly in accordance with the law and with due regard to the rights of the citizen concerned. His office gives him no right to prosecute the violator nor to mete out punishment for the offense. He shall, at all times, have a clear appreciation of his responsibilities and limitations regarding detention of the violator; he shall conduct himself in such a manner as will minimize the possibility of having to use force. To this end he shall cultivate a dedication to the service of the people and the equitable upholding of their laws whether in the handling of law violators or in dealing with the lawabiding.

Article 9. Gifts and Favors
The law enforcement officer, representing government, bears the heavy responsibility of maintaining, in his own conduct, the honor and integrity of all government institutions. He shall, therefore, guard against placing himself in a position in which any person can expect special consideration or in which the public can reasonably assume that special consideration is being given. Thus, he should be firm in refusing gifts, favors, or gratuities, large or small, which

can, in the public mind, be interpreted as capable of influencing his judgment in the discharge of his duties.

Article 10. Presentation of Evidence
The law enforcement officer shall be concerned equally in the prosecution of the wrong-doer and the defense of the innocent. He shall ascertain what constitutes evidence and shall present such evidence impartially and without malice. In so doing, he will ignore social, political, and all other distinctions among the persons involved, strengthening the tradition of the reliability and integrity of an officer's word. The law enforcement officer shall take special pains to increase his perception and skill of observation, mindful that in many situations his is the sole impartial testimony to the facts of a case.

Article 11. Attitude toward Profession
The law enforcement officer shall regard the discharge of his duties as a public trust and recognize his responsibility as a public servant. By diligent study and sincere attention to self-improvement he shall strive to make the best possible application of science to the solution of crime and, in the field of human relationships, strive for effective leadership and public influence in matters affecting public safety. He shall appreciate the importance and responsibility of his office, and hold police work to be an honourable profession rendering valuable service to his community and his country.



*E*thical
*C*limate
*A*ssessment
*S*urvey

An ethical climate is one in which the department's values are routinely articulated, supported, practiced, and respected. The ethical climate of an organization is determined by a variety of factors, including the following:
• Individual character of unit members,

• Policies and practices within the organization,

• Actions of unit leaders, and

• A variety of environmental and mission factors.

Leaders should periodically assess their organization's ethical climate and take appropriate actions, as necessary, to maintain the high ethical standards expected of public service organizations. This survey will assist you in making periodic assessments and in identifying the actions necessary to maintain a healthy ethical climate.

Self Assessment Exercise

1. How do Police Chiefs set the context for ethical behaviour in Law enforcement?

4.0 Conclusion

In the world of increasing population deviance and crime as well individual self control, no doubt ethical issues are very vital in the operation of law enforcement in order not to abuse powers. On the other hand offenders and the general public are also enlightened regarding the powers of police and other security agents complying and conforming to their directives.

5.0 Summary

This examines police ethics and relevant information on police ethics, ethical behaviours, the way and manner they are set, Policies and practices within law enforcement organizations, expected actions of unit leaders, and a variety of environmental and mission factors. It concluded with the submission that ethics is vital in the enforcement of laws on the part of the enforcers and compliance of offenders and the general public.

6.0 Tutor Marked Assignment

Write short notes on the following four documents guiding law enforcement

a. Law Enforcement Oath of Honor

b. Law Enforcement Code of Ethics

c. Law Enforcement Code of Conduct

d. Canons of Police Ethics

7.0 References/ Further Reading

IACP, *Leadership in Police Organizations*, Chapter 30, 2003.Arrington, R. 1983. "A Defence of Ethical Relativism." *Metaphilosophy* 14: 225–239.

Bunting, Harry. 1996. “A Single True Morality? The Challenge of Relativism.” Pp. 73–85 in *Philosophy and Pluralism*, edited by David Archard. Cambridge: Cambridge University Press.

Cook, John. 1999. *Morality and Cultural Differences.* New York: Oxford University Press.

Death Watch. 2002. “New Orleans: Recent History 1996.” Retrieved January 28, 2002 (www. hrw.org/reports98/police/uspo93.htm).

Felkenes, G. 1987. “Ethics in the Graduate Criminal Justice Curriculum.” *Teaching Philosophy* 10(1): 23–26.

Glover, Jonathan. 1999. “Capital Punishment.” Pp. 245–253 in *The Right Thing to Do: Basic Readings in Moral Philosophy* (2nd ed.), edited by J. Rachels. Boston: McGraw-Hill.

Hare, R. M. 1987. “Moral Conflicts.” Pp. 205–238 in *Moral Dilemmas*, edited by C. Gowans. New York: Oxford University Press.

Hinman, L. 1998. *Ethics: A Pluralistic Approach to Moral Theory.* Fort Worth, TX: Harcourt.

www.theiacp.org
(http://www.theiacp.org/profassist/ethics/index.htm)

UNIT 2

The Importance of Ethics in Criminal Justice

1.0 Introduction

Ethics, also known as moral philosophy, is a branch of philosophy concerned with the study of questions of right and wrong and how we ought to live. It is in this regard that Peter Singer (1995:174) wrote that:

> *To live ethically is to think about things beyond one's own interests. When I think ethically I become just one being, with needs and desires of my own, certainly, but living among others who also have needs and desires.*

Ethics involves making moral judgments about what is right or wrong, good or bad. Right and wrong are qualities or moral judgments we assign to actions and conduct. Within the study of ethics, there are three branches: *metaethics,* concerned with methods, language, logical structure, and the reasoning used in the interpretation of ethical terms, for example, what exactly does the term "good" mean; *normative ethics,* concerned with ways of behaving and standards of conduct; and *applied ethics,* concerned with solving practical moral problems as they arise, particularly in the professions, such as medicine and law. Ethics provides us with a way to make moral choices when we are uncertain about what to do in a situation involving moral issues. In the process of everyday life, moral rules are desirable, not because they express absolute truth, but because they are generally reliable guides for normal circumstances (Singer 1995: 175).

2.0 Objectives

The focus of this unit is on normative and applied ethics, particularly the exploration and analysis of ethical dilemmas and conflict situations that arise within the criminal justice system.

3.0 Main body

The Value of Ethics

The question usually is why do we need to study ethics? One view is that if we need to make a decision about a dilemma that confronts us, we can do so

without any knowledge of ethics. From this perspective, ethics is too abstract and theoretical and is not related to the practical world. Another view is that we need a system of rules and principles to help guide us in making difficult decisions when moral issues arise. If we cannot draw upon an ethical framework, we have to rely on emotion, instinct, and personal values, and these cannot supply an adequate answer to moral dilemmas. Among the reasons commonly given for studying ethics are the following:

1. Ethical considerations are central to decisions involving discretion, force, and due process that require people to make enlightened moral judgments.

2. Knowledge of ethics enables a person to question and analyze assumptions that are typically not questioned in areas of activity like business and politics. Questioning the criminal justice system should also be encouraged. This includes raising issues regarding such topics as the relationship between crime and justice, the role of law enforcement, the place of punishment, the limits of punishment, the authority of the state, the proper function of prisons, fairness in the workplace through creating a safe working environment, and equal opportunity.

3. The study of ethics increases sensitivity to issues of right and wrong and the right way to conduct oneself, and aids in identifying acts that have a moral content.

4. Only through studying ethics is it possible to define unethical behaviour. A full understanding of ethical behaviour demonstrates that it includes not only “bad” or “evil” acts, but also inaction that allows “bad” or “evil” to occur.

5. It is important to have the capacity to point to moral reasoning in justifying behaviour , and the study of ethics develops that capacity.

6. It is crucial that ethical decisions are made, and the study of ethics enables the development of tools that enhance ethical decision making.

7. Training in critical ethics helps to develop analytical skills and reasoning abilities needed to understand the practical as well as the theoretical aspects of the criminal justice system (Felkenes 1987).

8. Understanding ethics enables an appreciation of the complexities of acts that involve ethical issues and dilemmas.

9. Without knowledge of ethics, criminal justice professionals may be naïve about moral issues occurring within the criminal justice system.

10. The study of ethics helps criminal justice professionals quickly recognize the ethical consequences of various actions and the moral principles involved.

11. Within the criminal justice system, ethics is germane to most management and policy decisions relating to punishment and is the rationale used in making these decisions, such as whether to rehabilitate, deter, or impose just deserts. Examples of such management and policy issues include whether it is ethical to force someone to attend a treatment program against his or her will, and, given that the system of punishment is based on rehabilitation, whether it is ethical to send an offender to jail and not offer treatment programs to help him or her change behaviour in order to regain freedom (Felkenes 1987).

12. The criminal justice system comprises professionals who exercise power and authority over others, and who in some cases are authorized to use force and physical coercion against them. The law, or accepted standards of behaviour, impose ethical rules and responsibilities on these professionals. It follows that professionals in the criminal justice system must be aware of ethical standards in carrying out their functions. Ethics is crucial in decisions involving discretion, force, and due process, because criminal justice professionals can be tempted to abuse their powers (Felkenes 1987). In this unit, the value of the study of ethics by criminal justice professionals will become apparent as the criminal justice system is analyzed to reveal how decision makers sometimes fail to make the "right" choices, or deliberately act unethically in carrying out their functions. It will become clear that studying and applying ethics is a prerequisite for any competent criminal justice professional.

Normative Ethics

Normative ethics is fundamental to ethical decision making in the criminal justice system. A central notion in normative ethics is that one's conduct must take into account moral issues; that is, one should act morally, using reason to decide the proper way of conducting oneself. Essentially, ethics, in prescribing certain standards of conduct, gives us a way of making choices in situations where we are unsure about how to act. What are these standards of conduct and how do we decide what is right and wrong? Some argue that because standards of conduct and ways of doing things differ from society to society, there can never be one single standard for all people everywhere, and that we must make ethical decisions based on each situation. This approach to setting standards of conduct is called *ethical relativism.* Others argue that one set of ethical standards applies across all societies, and people have an obligation to do what is "known to be right"; that is, they argue in favour of *ethical absolutism.*

Ethical Relativism

Ethical relativists argue that what is morally right or wrong may vary in a fundamental way from person to person or from culture to culture. In other words, as Arrington (1983) argues, we cannot simply say that a moral judgment is true for all purposes, persons, and cultures—we can assert only that it is true for a particular person or social group. Relativism does not mean that we cannot criticize people of other cultures on moral grounds, but it does mean that when we say that a person in another culture did wrong or acted immorally, we must judge that person by the standards of that culture and not by our own (Cook 1999: 35). In other words, there are objective moral standards as long as right or wrong are used relatively. Holmes (1998: 163–164) discusses three forms of ethical relativism: ethical relativism, cultural relativism, and extreme or individual relativism. *Ethical relativists* agree that there is moral right and wrong, but contend that what is right for one person or culture may be wrong for another. *Cultural relativism* is a form of relativism that claims that moral beliefs and practices vary from culture to culture. It is important to understand, however, that cultural relativists do not argue that certain acts or practices are right or wrong in a particular culture. They simply note the differences. *Extreme or individual relativism* takes the position that moral beliefs and practices vary from person to person. In contrast to ethical absolutists (see the following section "Ethical Absolutism"), ethical relativists draw attention to factors such as moral diversity among different cultures, the varying state of morals in a particular society at different historical periods, and the fact that at any given time there is a high degree of moral disagreement within a particular culture. One example is the moral disagreement in the United States concerning abortion (Bunting 1996: 73).

Cultural Relativism

The proponents of *cultural relativism* argue that every society has a different moral code explaining what acts are permitted or not permitted. They argue that we cannot judge one moral code as being superior to another because there is no objective standard to apply to make such a judgment. In other words, the moral code that we, in the United States, subscribe to is not special; it is simply another moral code among many. If the moral code of a particular society determines that a certain act is right, then the act is right within that society. It is not for us to judge other people's conduct in other societies. We should be tolerant and avoid being judgmental. At first, the notion of cultural relativism seems to reflect the way many of us see the world; for example, we believe in tolerance and understanding and we recognize diversity in society. However, there are a number of objections to cultural relativism that show it cannot be viewed as a viable approach to ethical issues, including the following:

• There is the problem of identifying what constitutes a culture or society. For example, it is easy to imagine an isolated tribe in a far-off country as a separate culture with its own ethical standards and rules, but what of American culture? Although we may think of American culture as homogeneous, it is very diverse because many languages are spoken within it, and the various ethnic groups

that make up American society may well maintain their own ethical standards of conduct, which differ from those of the dominant culture.

• If this difficulty in identifying a culture or society exists, then it is easy to see that we may end up in a position where our own individual values, family background, education, or religion can determine ethical standards. In other words, cultural relativism can become transformed into a matter of individual ethics (individual relativism), where each person can claim that his or her moral standards are those that should apply to society and others.

• Cultural relativists are not able to explain which ethical standards should apply when cultures overlap. Cultures are no longer totally isolated from each other, and it becomes increasingly difficult to avoid interacting with other cultures. This raises the problem of deciding whose ethical standards are to apply.

• In all societies, standards of conduct change over time, and the cultural relativist is faced with the problem of acknowledging these changes while arguing that morality is relative to a culture. However, which values in which historical period should apply? On the face of it, the values applying in all periods have equal validity. For the cultural relativist, therefore, there is no overall standard to apply.

• A major problem with cultural relativism is that it operates as moral isolationism. This means that arguing that everything is relative tends to suggest this must be the end of the issue and debate must stop. It also suggests, in the view of Carol Gilligan (in Hinman 1998: 55), an attitude of "couldn't care less" because when we say that all things are relative, we are really saying we don't care about them. Therefore, cultural relativism fails to provide us with answers to issues, and in fact tends to close off debate altogether. Cultural relativism is closely associated with anthropology, and some even refer to it as an anthropological theory. Some philosophers argue that cultural relativism is in fact a methodology that requires that they adopt a nonjudgmental framework toward the culture they study, and therefore, as a methodological practice only, cultural relativism does not involve moral relativism (Cook 1999: Chapter 7; Ladd 1973: 2). However, other philosophers contend that cultural relativism contains elements of both methodology and a value system (Womack 1995: 48).

Ethical Absolutism

This view argues that there exists an eternal and unchanging moral law, the same for all people, at all times and places (Holmes 1998: 165). The absolutist believes that certain moral principles apply to all people everywhere, and that people can recognize or discover these principles and be guided by them in deciding the nature of their own conduct and in judging the conduct of others. Also, the ethical absolutist, being already aware of these principles, believes

himself or herself qualified to pass judgment on anyone (Cook 1999: 7). Absolutism is considered valid regardless of thought and feeling. This position is the opposite of relativism, in that there can be no consideration of other perspectives because it is argued that there is only one "true" perspective. An example of an absolutist position arises in arguments about capital punishment. As Jonathan Glover (1999: 245) points out, two absolutist views prevail on this question. One is emphatic that the murderer must be given the punishment he or she "deserves," which is death, and the other can see no justification for "judicial murder" under any circumstances. An absolutist would not change his or her view whether they opposed or supported capital punishment, whatever arguments were put forward by either side. Among the questions that arise from adopting an absolutist position include, "If there are universally accepted values, what are they?" and, "If universally accepted values exist, do they remain constant or do they change over time?" If there is disagreement about moral issues between societies, then how should we act? On the one hand, the ethical relativist will say we should not judge and there is no single truth that applies across societies and cultures. On the other hand, the moral absolutist will argue that one single truth must be applied across all societies and cultures, regardless of beliefs and values. In favor of ethical relativism, it can be said that it is correct in warning us against assuming that our ethical standards represent some absolute standard, because many, although not all, of our ethical standards apply only to our own society. Also, ethical relativism teaches us the value of an open mind, of tolerance, and of understanding. One way of resolving this disagreement about relative and absolute ethical standards is the notion of *ethical pluralism.*

Ethical Pluralism

Ethical pluralism argues that in most situations there are many truths rather than one single truth. Lawrence Hinman (1998: 67–68) contends that ethical pluralism allows us to adopt four principles to resolve conflicts between differing ethical standards. These principles are:

a. *The Principle of Understanding:* This requires that we fully understand and appreciate the meaning of ethical standards found in another culture from the perspective of that culture. For example, before making any judgment about an issue such as female circumcision, we should possess a full understanding of the history and cultural context of this practice as it applies in the many societies in which it is performed. We should recognize that a Western response to an issue of this nature is shaped and constructed by our own cultural values.

b. *The Principle of Tolerance:* This means accepting the existence of differences as opposed to denying any diversity in ethical standards. This principle therefore rules out an approach based on ethical absolutism.

c. *The Principle of Standing Up Against Evil:* Hinman argues that understanding and tolerance ought not to lead us to a position where "anything goes," as the ethical relativists argue, but rather, we should be prepared to stand up against what he calls "egregious moral wrongdoing," especially when such conduct affects the powerless and the marginalized of the world. An example of this kind of moral wrongdoing would be the crime of genocide, which is internationally recognized as a crime against humanity.

d. *The Principle of Fallibility:* This principle argues in favor of our own fallibility. We should always be prepared to learn from other cultures and to have our own moral shortcomings exposed. Most countries have prohibited capital punishment for children. However, in the United States, the Supreme Court has declared that states have the right to execute those as young as 16 years of age. The principle of fallibility would argue that the United States and its Court may not have chosen the correct ethical position on the issue of capital punishment and should be prepared to listen to the reasoning and experience of the rest of the world, which has outlawed it.

Other philosophers seem to agree with an approach that emphasizes ethical pluralism, which Kane (1996: 14–16) calls "openness." He stresses that a pluralistic point of view only suggests the possibility that other views are correct, but does not demonstrate that they are in fact correct. Pluralism challenges absolute values, but does not rule out their possibility. We can be open and tolerant to other points of view while still believing that some are better than others, even while we believe that only one is correct. Openness does not imply indifference; it only indicates recognition that we do not possess the truth and are willing to learn from others and to search for truths beyond our own limited point of view. Kane advocates an approach that assumes an attitude of openness to other points of view to allow others to prove themselves right or wrong. Cook (1999: 169) suggests an approach that sets aside an argument based on tolerance and that instead advocates taking cases one by one and examining them in light of the details of each particular case. He therefore suggests that the question of whether we ought to interfere with the practices of another culture is not a philosophical question but a practical moral one. The examination of a particular case means understanding the nature of the problem, what considerations would be relevant to a solution, and what a "right solution" would be. This seems to parallel Hinman's point that there must be a full understanding of the cultural context of a particular case before any attempt is made to resolve conflicts among differing ethical standards.

Self Assessment Exercise

a. How is ethics defined?

b. Why is it important for criminal justice professionals to study ethics?

c. Explain how applying ethical approaches helps criminal justice professionals make appropriate and "correct" decisions.

4.0 Conclusion

Ethics no doubt gives a broad perspective of human existence and diversity. It broadens the minds provides professionals in security studies better understand of how best to make moral choices when one is uncertain about what to do in a situation involving moral issues. A firm grip of ethics is therefore necessary not only in criminal investigation but also in law enforcement.

5.0 Summary

The focus of this unit is on normative and applied ethics, particularly definitions, branches and values of ethics as a vital component in dispensing judgement and for professionals in the criminal justice system. It examines Normative Ethics as fundamental to ethical decision making with a central notion that one's conduct must take into account several moral issues; that is, one should act morally, using reason to decide the proper way of conducting oneself. It is in this view that one should expect that fundamentals differ from persons and cultures. This brings about the concept of Ethical Relativism on one hand and others such as the concepts of ethical Absolutism and pluralism showing that there exists an eternal and unchanging moral law, the same for all people, at all times and places vis-à-vis Ethical Pluralists argument that in most situations there are many truths rather than one single truth about morality which should form the basis of life and decision making. .

6.0 Tutor Marked Assignment

Discuss the concept of Normative Ethics in relation with:

a. Ethical Pluralism
b. Ethical Absolutism
c. Ethical Relativism

7.0 References/ Further Reading

Arrington, R. 1983. "A Defence of Ethical Relativism." *Metaphilosophy* 14: 225–239.

Bunting, Harry. 1996. "A Single True Morality? The Challenge of Relativism." Pp. 73–85 in *Philosophy and Pluralism*, edited by David Archard. Cambridge: Cambridge University Press.

Cook, John. 1999. *Morality and Cultural Differences.* New York: Oxford University Press.

Death Watch. 2002. "New Orleans: Recent History 1996." Retrieved January 28, 2002 (www. hrw.org/reports98/police/uspo93.htm).

Felkenes, G. 1987. “Ethics in the Graduate Criminal Justice Curriculum.” *Teaching Philosophy* 10(1): 23–26.

Glover, Jonathan. 1999. “Capital Punishment.” Pp. 245–253 in *The Right Thing to Do: Basic Readings in Moral Philosophy* (2nd ed.), edited by J. Rachels. Boston: McGraw-Hill.

Hare, R. M. 1987. “Moral Conflicts.” Pp. 205–238 in *Moral Dilemmas*, edited by C. Gowans. New York: Oxford University Press.

Hinman, L. 1998. *Ethics: A Pluralistic Approach to Moral Theory.* Fort Worth, TX: Harcourt

Brace. Holmes, Robert. 1998. *Basic Moral Philosophy* (4th ed.). Belmont, CA: Wadsworth.

Kane, R. 1996. *Through the Moral Maze: Searching for Absolute Values in a Pluralistic World.* Armonk, NY: North Castle Books.

Ladd, John. 1973. *Ethical Relativism.* Belmont, CA: Wadsworth. “92nd death row inmate freed since ’73: Louisiana.” January 5, 2001. *New York*

Times. Retrieved January 2002 (www.truthinjustice. org/no92.htm).

Rachels, J. 1991. “Subjectivism.” Pp. 432–441 in *A Companion to Ethics,* edited by P. Singers. Cambridge, MA: Blackwell Press.

Singer, Peter. 1995. *How Are We to Live? Ethics in an Age of Self-Interest.* Amherst, NY: Prometheus Books.

Womack, Mari. 1995. “Studying Up and the Issue of Cultural Relativism.” *NAPA Bulletin* 16: 48.

UNIT 3
POLICE ETHICS: A Case Study of Turkey

1.0 Introduction

The personnel of official law enforcement agencies such as the police and the gendarmerie have authorities and responsibilities that other public personnel do not. These are important powers that limit civil liberties, such as stopping, searching, asking for identification, confiscation, apprehending, using force, and interrogation. The performance of these duties has significant effects on people's quality of life, and especially on civil liberties and social life. Taking into account the degree of discretion allowed to security personnel to enforce the law, it becomes clear that there is a need for a code of professional ethics, in addition to existing legislation, in order to increase the quality of the service they provide. In this light, in this section questions such as 'what are police ethics,' 'to which security personnel do police ethics apply,' and 'why is a code of ethics necessary' will be considered. The section will also address the sources of ethical rules and their relation to police ethics, social morality and religious beliefs. Finally, the relationship between police ethics and professionalism will be addressed. Emphasis will be made on the necessity of compliance with the code of ethics by all full-time official and private security personnel currently active in the field of internal security services.

2.0 Objectives

Students are expected to

1. Understand the concept of police ethics, what they are and to whom do they apply.

2. Secondly this unit material why police ethics, source of ethical values and police ethics and professionalism.

3.0 Main body

The term 'police ethics' is a shorter phrase whose full meaning is actually 'professional policing ethics.' The term does not only cover the members of the police organization, but also the members of all other organizations providing internal security services, such as the gendarmerie, coast guard, and even

private security organizations. In Turkey, these services are being provided by three separate public organizations, the police, the gendarmerie, and the coast guard. Therefore, police ethics can also be referred to as 'law enforcement ethics;' a term that is not commonly used in everyday speech, but which is relevant for all internal security personnel. The term 'law enforcement ethics' includes, without exception, all security personnel. In this book, the term 'police ethics' is mostly used and is meant to include all organizations providing internal security services. Although the *European Code of Police Ethics* (ECPE) produced within the Council of Europe (CoE) involved the participation of gendarmerie officials from countries such as France and Spain, it was titled *European Code of Police Ethics*. As a result, the document addresses not only the police, but also gendarmerie organizations providing internal security services in European countries. Moreover, the ECPE was translated into Turkish and published by the Turkish Gendarmerie. The fact that these principles have been included in the book *Jandarma Eti¤i* (Gendarmerie Ethics) (2002) published by the gendarmerie demonstrates most clearly that police ethics includes gendarmerie ethics. In short, in order to determine which organizations are covered by the ECPE, the service provided rather than the *organizational structure* of the internal security unit has to be taken into account. While the police, one of the official law enforcement agencies, is under the control of the political authority and is organized as a semi-military institution, the other two, the gendarmerie and the coast guard, are organized in a completely military manner. However, regardless of the organizational structure of the units, all internal security services in democratic governments are defined as 'policing.' Therefore, the term 'police ethics' used in this book addresses all organizations that provide *internal* security services and, therefore, practice policing, not just those that have the organizational aspects and titles of the law enforcement agencies.

3.1. Why police ethics? One of the reasons why a code of ethics addressing security personnel is needed is the insufficiency of internal legal arrangements in controlling their actions. For this reason, ethical rules prepared and accepted by the members of this profession are needed in addition to existing legal arrangements. The healthier operation of security services and the minimization of human rights abuses depend on the establishment and acceptance of professional ethical principles and rules. It is obvious that it is not possible to control the behaviors and actions of the members of any given profession through laws that entail penal sanctions. While legislation has primarily penal sanctions, ethical rules have more professional, conscientious sanctions. In places and cases where the enforcement of the law is under the enforcement personnel's own initiative, the most effective element is professional consciousness, conscience, and ethics (Kleinig, 1996). It is a reality that the security personnel whose main duty is to enforce the law have more freedom in choosing whether to obey the law or not. Therefore, professional ethical rules prepared by security members and addressing their conscience will be more

effective in controlling the actions and behaviours of the police than just legislation.

In short, laws by themselves are not sufficient to control the behaviours of law enforcement personnel and institutions. The healthier performance of security services and the minimization of human rights abuses require the establishment of professional ethics in addition to legislation. For this reason, professional ethical rules prepared by parties representing many sectors of the society, and led by the members of the profession, are needed. Police personnel's values and perceptions of events are largely a product of the structure of the society to which they belong, the pre-professional training they receive, their work environments, and social lives. It is impossible to deny the impact of the society in which security personnel are born into and brought up on their moral and religious values. Although the ECPE prepared under the Council of Europe was prepared as a secular document, it is natural that certain social values pre-exist in the subconscious of the persons preparing it. However, the committee members made a special effort to ensure that the prepared document covers universal principles transcending Europe, instead of just reflecting Europe's social and cultural values.

3.2. By whom and how was the ECPE prepared?

High-level police officers, social scientists, jurists, and representatives of nongovernmental organizations participated in this study, which began towards the end of the 1990s and was finalized in the 2001 under the Council of Europe. The preparation of the ECPE took place in an overall democratic and scientific environment. Each member of the committee was given the chance to express her/his opinions and ideas on behalf of her/his country and society. The committee's studies represented the problems and reflected the opinions of security personnel at every level, not only high-level officials and bureaucrats. In particular, the problems of police officers - lower - and middle-level personnel providing services defined as 'street policing' - found a place. By ensuring the participation of personnel from every level in preparation of the document, the resulting ethical code was made more acceptable to non-ranked police officers. In short, the study was not only prepared by high-level security personnel but incorporated the contributions of all parties concerned. The committee facilitated the contributions of certain non-governmental organizations such as human rights organizations, as well as of law and social science academics. The sixth and last meeting took place in Strasbourg between 28 – 30 March 2001, where the document was finalized and presented to the police organizations of all member countries as a recommendation document.

3.3. Ethical Values

The source of ethical values and rules is an issue discussed by social scientists, especially philosophers. The crux of the matter is whether the source of ethics

is *human nature* or *socialization*. In other words, is it *nature* or *nurture* that defines them? Morality, related to the word 'creation,' implies that the good values of humans result from their nature. According to the opposite opinion, while ethical values are produced by humans, they are a product of their nurture, and not of their nature. This approach, which perceives of ethical principles as the product of the individual's socialization processes, argues that these principles are more universal compared to moral principles, regardless of their source. According to this opinion, moral rules are local and relative, whereas ethical rules are universal. On the other hand, human properties are more universal than the properties a person achieves through socialization. Apart from some physical details, such as skin-color, hair-color, and height, people the world over share similarities. People's socialization is more variable and relative compared to their physical properties. People can produce different, even conflicting ethical rules, as a result of their socialization in different societies and historical periods. The socialization of individuals is more diverse and contingent compared to their physical aspects.

People growing up in different environments and under different conditions accordingly present different lifestyles and values. In this case, morality, which includes the notions of 'nature' and 'good things' - and, which as used in Turkish comes from the Arabic word meaning creation - will be more universal compared to the ethical principles that humans will produce as a result of social relations. In short, socialization processes that lead to differences and the resulting social morality or professional ethical principles will be more local compared to the universal values that are allegedly inherent in human beings. There may be a direct or indirect relationship between professional ethics and religious beliefs. Religion is one of the oldest existing social institutions, and all people are influenced by religion to a lesser or greater degree. For this reason, ethical rules of a profession cannot be thought of as completely independent of the moral principles of the belief system to which the members of that profession belong or in which they live. Whether the source of ethical values is a person's nature and beliefs or her/his socialization, it is natural, even inevitable, that there will be a hidden or distinct relationship between the general moral rules of a society and the ethical rules of any given profession. Instead of completely rejecting or excluding the social moral principles of a society, those principles can be accepted as a foundation on which professional ethical rules can be built when establishing the ethical code of a profession. Ethical rules taking the sensibilities of different belief systems into account will have secular characteristics. In addition, they will be more comprehensive than ethical rules established according to the sensibilities of a single belief system.

This sensitive balance was maintained very well in the preparation of the ECPE. Although the resulting study was prepared as a secular document, it has taken into account different belief systems and lifestyles. The emphasis on the secular character of the document aims to avoid giving the impression that the

document was prepared in accordance with moral values of any one particular religion; and it does not mean that the document is devoid of any traces of moral principles of any society or religion. For instance, it will not be convincing to claim that the ideas of a person who accepts as ethical principles not to profit unfairly or to abuse one's power are not based on her/his moral and religious beliefs. The influences of religious beliefs or social moral principles on ethical principles can be direct, or they can be in the form of values embedded in the subconscious of the individual. When the relationship between morality and ethics is considered in this way, a professional code of ethics can be conceptualized as the adaptation of social and religious principles in accordance with the needs and priorities of different professions. For this reason, the fact that the ECPE is a secular document does not mean that none of the ethical principles in this document has any relation to religious or moral principles.

The secular nature of the document is emphasized in order to express that it was not shaped solely by beliefs and values of Christianity, which is the dominant religion in Europe. The ECPE's introduction emphasizes that the concept of ethics is different than the concept of morality. However, the introduction also mentions the relationship between the terms 'ethics' and 'morality.' It has been pointed out that ethics is a kind of reflection of the concept of morality, as it is used in everyday speech, on professional policing actions. In other words, professional ethics is the reflection of morality as a concept that is related to an individual's values at a professional level. It is known that beliefs and cultural systems of different societies have important effects on shaping the understanding of morality in those societies. The understanding of morality in European societies is also naturally formed according to Christian beliefs. So as not to give the impression to non-Christian Europeans that a morality based on Christian beliefs is being imposed on them, the more secular term 'ethics' is used instead of 'morality,' which is affiliated with religion. Thus, care was taken so that the ECPE prepared under the CoE would be a secular document rather than a religious or a moral one. However, the particular and insistent stress on the difference between ethics and morality throughout the committee's studies compels one to think that there can be a larger or smaller relation between the two concepts. Otherwise, a non-existent issue would not have been discussed so insistently. In this case, we can ponder the persistent denial of this link. If the issue is considered in depth, two reasons are revealed.

The first of these reasons is that the committee members wished to keep the concept of ethics distinct from religion, and especially from the concept of morality as related to Christianity. Although this study was prepared by the Council of Europe, the resulting code did not only concern the police forces of European countries. Some countries whose inhabitants identify themselves predominately as Muslims, such as Turkey and Azerbaijan, were also represented in the committee. Furthermore, minorities with various religious

affiliations live in every European country, in numbers that cannot be underestimated. European countries no longer consist of a single race, religion, or culture as in the Middle Ages. Therefore, the ethical code produced by the committee intended to address both religious minorities living in Europe as well as people living in predominately Muslim countries. In conclusion, the sensibilities of non-Christian communities such as the Turks living in Europe, and of Turkey - a member of the Council of Europe and a country with a predominately Muslim population – were taken into consideration. Secondly, other religious minorities living in Europe and some non-European countries might not have accepted a code that explicitly and predominantly contains moral values shaped according to Christian beliefs. It can be said that this idea is behind the elaboration of the concept of ethics as particularly distinct from morality. It was out of a desire not to impose moral values reflecting primarily Christian beliefs on all people under the guise of professional ethics, or to leave such an impression. Only this kind of an approach would have been appropriate to the spirit of the prepared ethical code. According to the committee, the ethical code prepared in this way will be a document accepted by the various religious, ethnic, social, and cultural minorities living in Europe. The committee is of the opinion that such acceptance will be possible only when the concept of ethics is based on humanity, and not on any particular religious belief.

3.4 POLICE ETHICS AND PROFESSIONALISM

The issue of *how* and *who* will control the personnel providing security services has existed since the time when these services first appeared. The need for a professional ethics code in guiding the actions of security personnel is a result of such efforts. There have been other police ethics studies in Western countries prior to the *European Code of Police Ethics* (Kleinig, 1996). The book *The Principles of Policing and Guidance for Professional Behavior*,1 published in 1985 by the British police, is one of the first publications that established a relationship between ethics and professionalism. Professional ethics education is also known to have existed in the history of Turkish security services (Bal and Beren, 2003: 64). There are documents showing that Police Ethics classes existed in Turkish police education in the last periods of the Ottoman State (1910) and in the first years of the Republic of Turkey (1939). Among them is a book titled *Polis Efendilere Mahsus Terbiye ve Malumat-› Meslekiye* (Professional Training and Information for Policemen) published by the educator and police chief ‹brahim Feridun in 1910 in Istanbul. This book was used as a textbook in police schools at that time. Upon examining the book, it becomes obvious that modern principles such as transparency, accountability, community policing, and service found inside the contemporary *European Code of Police Ethics* also appeared in that book. However, for some reason police ethics courses were not offered in preprofessional or professional institutional training of the Turkish police in later years.

Towards the end of the 1990s, police ethics courses started to be offered again in formal police education in Turkey, in parallel with police ethics studies carried out under the Council of Europe. In reality, the acceptance of a profession as a professionally practiced field must be accompanied by the development of some professional ethics principles. Such a connection also exists between police ethics and professional policing. If policing is a service branch that must be practiced professionally, there must be ethical rules covering the rights and wrongs of this profession. These ethical rules are defined by the members of that profession, who are its representatives and the providers of its services. Their own colleagues punish those who do not comply with those rules according to ethical rules. This is one of the musts for a field to be considered professional. In other words, professionalism requires compliance with ethical rules. A police officer who works in accordance with ethical rules is a professional police officer. The idea of professionalism does not merely bring some additional responsibilities upon the members of a profession. In this light, the code of police ethics should not be viewed as a document that restrains security service personnel and makes their task more difficult. The existence of code of ethics and compliance with it will ensure that the people who are providing this service and those who receive it will be in a healthier relationship. Security personnel performing their duties with professionalism will internalize the ethical code of their profession and will transform it into normal and routine behavioural patterns over time. Moreover, a professional individual does not perceive acting ethically as something extraordinary that should be rewarded. Ethical behaviour will not only benefit those to whom it is directed, but will also give happiness to the person who acts ethically. In fact, security personnel who practice proper behaviours in line with professional principles will live a more peaceful life. They will at the same time extend this happiness to their environments. Those who violate the law and ethical codes will make their colleagues, their close environments, family members, and even themselves unhappy. In short, individuals who provide services professionally and in accordance with ethical codes will not benefit only the society they are serving; individuals who act ethically in their professional lives also will be happier in their private and family lives. For this reason, security personnel should not view ethical rules and principles as an additional arrangement that limits and controls them. They should accept compliance with the ethical code as benefiting both themselves and others, and as a requirement of their professionalism.

Self Assessment Exercise

What is the source of ethical values?

4.0 Conclusion

There is a close relationship between professionalism and professional ethics. Being a professional member of a service sector requires willingness to comply with that profession’s ethical code. This requirement covers all personnel that

have chosen internal security as a full-time service area. For this reason, although the ECPE is a document prepared for official security personnel, personnel of private security organizations that, according to recent legislation, assist official security organizations in providing security services are also bound by these ethical principles. In short, since their duty is to provide security services, it is necessary and useful for these organizations and their personnel to become aware of and adopt basic ethical rules of security service established for official security personnel.

5.0 Summary

This unit highlight some of the important powers that limit civil liberties, such as stopping, searching, asking for identification, confiscation, apprehending, using force, and interrogation. From which The term 'police ethics' was described as a shorter phrase whose full meaning is actually professional policing ethics. Similarly the reason for code of ethics in policing revealed that the need for control in the actions of police personnel is paramount in the light of existing legal arrangements which characterised the police as professionals..

6.0 Tutor Marked Assignment

1. What is police ethics?
2. What are the reasons for ethics in any organisation?

7.0 References/ Further Reading

Bryden, A. and Fluri, H. P. (Eds) (2003) *Security Sector Reform: Institutions, Society and Good Governance*, Baden-Baden: Nomos Verlagsgesellschaft.

Hanggi, H. Winkler, T. H. (2003) *Challenges of Security Sector Governance*, Geneva Center for the Democratic Control of Armed Forces.

Lynch, G. W. (1999) *Human Dignity and the Police: Ethics and Integrity in Police Work*, Illinois: Charles C Thomas.

Munteanu, T. (2005) 'Reforming the security sector: The experience of the SEE and the Black Sea region', paper presented to the Halki International Seminars 2005 – on *Security Sector Reform in South Eastern Europe and the Mediterranean: Lessons and Challenges*, 7-11 September 2005, Greece.

Qatarneh, Y. (2005) 'Civil-military realations and security sector reform in the Arab world', paper presented to Halki International Seminars 2005- *on Security Sector Reform in South Eastern Europe and the Mediterranean: Lessons and Challenges*, 7-11 September 2005, Greece.

UNIT 4
Natural Law and Ethical Dilemmas

1.0 Introduction

In looking at the origin of ethics, some ask whether natural law is the origin. The idea of natural law is that underneath the diversity of human cultures and beliefs about what is right and wrong, we can identify some factors that are common to our human nature. The notion of natural law was a favourite of ancient thinkers like Plato and Aristotle, who sought to identify universal traits of human nature, with the aim of finding common goals or ends that would bring human fulfilment or happiness (Kane 1996: 46). This pattern of looking for natural laws continued into the medieval and later periods of Western culture. Natural laws are said to be laws that govern human behaviour and define the right way to live. They are said to be "natural" because they are thought of as incorporating human nature and the goals that humans naturally seek. In effect, natural law represents a search for moral absolutes that define what is "normal" and "natural." For example, despite more progressive and inclusive modern attitudes toward homosexuality, some still argue that practicing homosexuality is "unnatural" because it is contrary to human nature. Nowadays, natural law arguments have tended to gravitate towards arguments in favour of human rights.

2.0 Objectives

The focus of this unit is to examine natural law, normative and applied ethics, particularly in relation to decision making the exploration and analysis of ethical dilemmas and conflict situations that arise within the criminal justice system.

3.0 Main body

Is law a source of ethical standards, and what is the relationship between law and ethics? It is important to understand that ethics and law are distinct categories. By law, we generally mean legislation, statutes, and regulations made by states and by the federal government on a host of subjects for the public good and public welfare. Laws do not, and are not intended to, incorporate ethical principles or values, but sometimes ethical standards will be reflected in laws. For example, both morality and the law prohibit the act of

murdering another human being. Similarly, legislation regulating the legal profession or other professions may give legal effect to certain professional codes of conduct. It is possible to argue, therefore, that codes of conduct regulating legal practice have the force of law. However, on a whole range of subjects from business practice to driving a vehicle, laws do not set ethical standards. It is important to appreciate, therefore, that ethical standards are not necessarily written down in the form of laws or other rules, but represent the collective experience of a society as it regulates the behavior of those who make up that society. The fact that an ethical standard is not repeated or copied in a law does not affect the validity of that ethical standard. However, where ethical standards are incorporated into law, such as the right to choose an abortion, although people must obey the law, they are not necessarily required to hold the same ethical beliefs expounded by that law. Sometimes laws can conflict with ethical standards. For example, laws promoting apartheid in South Africa and slavery in the United States were both clearly in violation of ethical standards relating to the dignity of the person, but were nevertheless lawful and were expected to be obeyed when in force. From time to time, a mass movement develops against a particular law or set of laws, reflecting a section of public opinion that claims that the law is wrong and should be repealed. Where there is a deliberate disregard of the law by those protesting its wrongness, the result can be acts of civil disobedience. For example, in India during the British colonial period, Gandhi advocated and practiced civil disobedience to British laws because he and his followers wanted an end to the colonization of their country. Similarly, in the United States, activists in the civil rights movement deliberately flouted laws that were racially discriminatory, and civil rights workers were prepared to be arrested and jailed in pursuit of equal treatment for all citizens.

ETHICAL DILEMMAS

Ethical questions and issues arise for all people, not just for professionals in the criminal justice system, or professors who teach ethics, or members of the clergy. We may all have to make decisions involving ethical issues in our daily and professional lives because, as we have noted, ethical issues are concerned with questions of right and wrong and how we ought to act. For example, we might apply for a job, and in order to be considered for the position, we may have to decide whether to hide the fact that we were fired from a previous job for misconduct. In other words, we have to decide whether to lie to promote our own career interests or whether to reveal the truth. Another instance may arise as we walk down the street and see a person who is apparently homeless, panhandling from passersby. The ethical dilemma here is whether we should act to help the poor and needy or just pass by and give nothing. We will have to make ethical decisions in our day-to-day lives, so it is helpful to recognize when an issue involves ethical considerations, and then to be able to apply a knowledge of ethics, including ethical terminology and concepts, in making our decision about what to do.

A number of ethical approaches can be taken in making a decision about an ethical issue, and you will see in the following chapters that no one approach is the "correct" one; rather, different approaches are equally valid in ethical terms. The approach we adopt to an ethical issue will frame and give meaning to any decision we make, and can be used to justify and validate our actions. Of course, it is always possible to abandon the responsibility for making an ethical decision. We might decide that we will simply follow the dictates of others rather than applying our own mind to a particular ethical issue. For example, during World War II, many war crimes were committed by members of the Nazi Party who claimed they were simply following orders in committing those crimes. In effect, they abandoned their responsibility to make an ethical decision not to kill or murder, and opted instead to obey unethical and inhumane directions. Similar situations may arise in the criminal justice system. For example, a prosecutor may have to decide whether to seek the maximum penalty against an accused under three-strike legislation. If he or she does decide to seek the maximum, the result may be that the accused will be incarcerated for the rest of his or her life. A prosecutor may decide to act ethically and fully weigh this issue in light of the facts of the case and the nature of the crime committed.

Alternatively, he or she may choose not to follow that process and may simply take the position that the law reflects public opinion, and that he or she should always exercise discretion so as to impose the full penalty provided by the law. When we decide to accept responsibility and make a decision involving ethical considerations, we are faced with a personal ethical dilemma. A personal ethical dilemma can be contrasted with an ethical issue. The latter is usually an issue of public policy involving ethical questions. Examples of such issues include the morality of capital punishment, whether to incarcerate more people or use alternative sanctions for convicted offenders, and other important social issues. A further distinction between ethical dilemmas and ethical issues is that an ethical dilemma is the responsibility of an individual and requires a decision to be made. Ethical issues, on the other hand, being broad issues of social policy, do not require individual decision making beyond the decision of whether one is in favour of, or opposed to, a particular social issue. However, the fact that ethical issues do not require most individuals to decide the issue does not mean that an individual is helpless to influence the public debate on a social issue.

Ethical dilemmas are important in the criminal justice system because criminal justice professionals are often faced with having to make decisions that involve ethical issues. Much of the material in this unit concerned with ethical practices in the criminal justice system will focus on ethical dilemmas faced by criminal justice professionals, and will analyze options in light of ethical theories and any relevant rules and regulations. How do we recognize when a dilemma is an ethical dilemma as opposed to merely a dilemma? An ethical dilemma arises only when a decision must be made that involves a conflict at the personal,

interpersonal, institutional, or societal level, or raises issues of rights or moral character. What process is followed in resolving an ethical dilemma? Hare (1987) argues that we initially use an *intuitive* level of moral thinking when we consider ethical dilemmas. This provides us with relatively simple principles derived from our upbringing and past experience of decision making. *Critical thinking* is another process of thinking about moral decisions; in contrast to intuitive thinking, critical thinking applies principles established by philosophy and moral concepts, and is therefore non-intuitive. In making moral judgments when faced with moral dilemmas, we may initially apply an intuitive form of thinking, relying on our intuition to identify possible courses of action to make the decision. However, we are likely to find that our intuitions do not adequately equip us to make moral decisions and that critical thinking is required. Consider the following scenario:

> A newly recruited correctional officer, Tom, overhears three other correctional officers, Fred, Bob, and Charlie, discussing arrangements to assault an inmate, Raymond, who has previously attacked another correctional officer, a close friend of the three officers.

Box 1: AN HYPOTHETICAL EXAMPLE

Tom is faced with a dilemma: whether or not to prevent the attack on Raymond. His dilemma is an ethical dilemma because if he does act, this will involve a conflict between himself and Fred, Bob, and Charlie. It is also an ethical dilemma because it raises issues of rights and morality; that is, the right of Raymond to safety and security even in prison, and the morality of allowing a person to be assaulted other than in an act of self-defense. In order to resolve his ethical dilemma, Tom will need to pursue a process of analysis resulting in a decision. The following process is intended to provide Tom with a method for reaching his decision:

- He will identify the fact that he is faced with an ethical dilemma and state the dilemma clearly.

- In his mind, he will collect the facts and circumstances of what he overheard so that he is quite clear about what he heard, the identities of those involved, and all other relevant information.

- He will collect all the facts and knowledge relevant to the decision, including his own values about the issue, and the values of his workplace. He will consider his own position at the prison as a newly trained officer and the consequences of reporting the incident and of not reporting it.

- This is an ethical dilemma, so he will call to mind his knowledge of ethical principles and theories with the aim of applying those ethical approaches to his possible courses of action.

- Tom will now identify his available options for action. First, he could intervene in the situation by informing his supervisor of the conversation he overheard. This action will be based on his responsibility to ensure the safety and security of all inmates and to enforce the policies and rules of the institution. Second, he could choose to ignore the conversation because of his loyalty to his fellow officers and his need in the future to receive their assistance and support when carrying out his duties. Third, he could choose to intervene by talking to the officers involved in an attempt to prevent the misconduct, wit the aim of minimizing the harm for all involved parties. Tom must support each alternative action with reasoning derived from ethical principles in order to give credibility to his choice of action.

- Tom will make his decision based on his analysis of the dilemma after applying the ethical approaches to each course of action. He will choose the option that for him is the most ethically appropriate. In other words, after considering the choices according to this process, he will decide, “This would be the right thing for me to do.” He therefore resolves his

ethical dilemma by making an ethical decision and acting on that decision.

From the hypothetical examples above it is obvious that Tom's process for making an ethical decision was straightforward. However, making an ethical decision may involve factors such as one's personal values, personal priorities, or how a particular decision might affect friends or even strangers. Therefore, the most ethical choice is not always clear. To act ethically is not simply a matter of deciding what is right and wrong in advance and stubbornly sticking to that position. Since there are many gray areas where there are no specific rules, laws, or guidelines laid out in advance, it is not always easy to know which decision is the most ethical choice. In addition, if we are to act in an ethical way we have to justify what we do, and the justification must be

sufficient that it could in principle convince any reasonable human being. As Rachels (1991: 438) puts it,

> . . . a moral judgment . . . must be supported by good reasons. If someone tells you that a certain action would be wrong, for example, you may ask why it would be wrong, and if there is no satisfactory answer, you may reject that advice as unfounded. In this way, moral judgments are different from mere expressions of personal preference. . . . moral judgments require backing by reasons, and in the absence of such reasons, they are merely arbitrary.

Hare (1987: 218) argues that moral judgments must be able to be applied universally. According to this principle, similar actions ought to be judged similarly unless there are morally relevant differences between them. For example, if I judge it wrong for you to cheat in examinations, I must be prepared to say that it is wrong for me as well, unless I can explain how my situation is different from yours in a morally relevant way (Holmes 1998: 151). Thus, the principle does not say whether you should cheat, but it does require that whatever you do, you must be consistent. Singer (1995: 175) expands this notion somewhat by arguing that when thinking ethically, I ought to consider the interests of my enemies as well as my friends, and of strangers as well as my family. If, after I have fully taken into account the concerns and preferences of all these people, I still believe that a particular action is better than any alternative, then I can honestly say that I ought to do it. What weight do we give to our *personal values* when making ethical decisions? By values, we mean what individuals care about and what they think is important. This can include such things as people's desires, such as social approval and what they enjoy, such as sports or music, their goals or purposes, their ideas of happiness or success, and their highest ideals. Each person develops a set of values which forms his or her value system. We often assume that our values are similar; however, we may define values differently than others. For example, we may have different definitions of what constitutes a "family" but we may all share "family" as a value. Even if we do have similar definitions of values, we often prioritize them differently. Thus, one person might give the value of "freedom" a higher priority than the value of "preservation of life." Another may prioritize the value of "loyalty" higher than "personal freedom." The fact that we may order our values differently explains why our thinking about ethical decisions differs from others, and why we arrive at different conclusions.

Self Assessment Exercise

1. How do we recognize when a dilemma is an ethical dilemma as opposed to merely a dilemma?
2. What process is followed in resolving an ethical dilemma?

4.0 Conclusion

Once again the relevance of ethics was brought to bear as all humans have the capacity to take decisions and what, when and how these are taken becomes an ethical issue in our daily lives at work or home. Ethical dilemma therefore arises only when a decision must be made that involves a conflict at the personal, interpersonal, institutional, or societal level, or raises issues of rights or moral character.

5.0 Summary

This unit discusses natural law and the ethical dilemmas individuals face in decision in everyday life activities. The importance of Ethical dilemmas in the criminal justice system cannot be over emphasised because criminal justice professionals are often faced with having to make decisions that involve ethical issues. A hypothetical examples of one of these dilemmas was highlighted as in the case of the correctional officer (See Box I).

6.0 Tutor Marked Assignment

1. What is the relationship between law and ethics?
2. Is law a source of ethical standards? Discuss.

7.0 References/ Further Reading

Arrington, R. 1983. “A Defence of Ethical Relativism.” *Metaphilosophy* 14: 225–239.

Bunting, Harry. 1996. “A Single True Morality? The Challenge of Relativism.” Pp. 73–85 in *Philosophy and Pluralism*, edited by David Archard. Cambridge: Cambridge University Press.

Cook, John. 1999. *Morality and Cultural Differences.* New York: Oxford University Press.

Death Watch. 2002. “New Orleans: Recent History 1996.” Retrieved January 28, 2002 (www. hrw.org/reports98/police/uspo93.htm).

Felkenes, G. 1987. “Ethics in the Graduate Criminal Justice Curriculum.” *Teaching Philosophy* 10(1): 23–26.

Glover, Jonathan. 1999. “Capital Punishment.” Pp. 245–253 in *The Right Thing to Do: Basic Readings in Moral Philosophy* (2nd ed.), edited by J. Rachels. Boston: McGraw-Hill.

Hare, R. M. 1987. “Moral Conflicts.” Pp. 205–238 in *Moral Dilemmas*, edited by C. Gowans. New York: Oxford University Press.

Hinman, L. 1998. *Ethics: A Pluralistic Approach to Moral Theory.* Fort Worth, TX: Harcourt

Brace. Holmes, Robert. 1998. *Basic Moral Philosophy* (4th ed.). Belmont, CA: Wadsworth.

Kane, R. 1996. *Through the Moral Maze: Searching for Absolute Values in a Pluralistic World.* Armonk, NY: North Castle Books.

Ladd, John. 1973. *Ethical Relativism.* Belmont, CA: Wadsworth. “92nd death row inmate freed since ’73: Louisiana.” January 5, 2001. *New York*

Times. Retrieved January 2002 (www.truthinjustice. org/no92.htm).

Rachels, J. 1991. “Subjectivism.” Pp. 432–441 in *A Companion to Ethics*, edited by P. Singers. Cambridge, MA: Blackwell Press.

Singer, Peter. 1995. *How Are We to Live? Ethics in an Age of Self-Interest.* Amherst, NY: Prometheus Books.

Womack, Mari. 1995. “Studying Up and the Issue of Cultural Relativism.” *NAPA Bulletin* 16: 48.

UNIT 5
Law Enforcement Code of Ethics and the Use of Authority

1.0 Introduction

The law gives police extraordinary powers and, at the same time, circumscribes those powers in a manner that ensures that they are not abused. This form of expression of the doctrine of the separation of powers not only ensures that power is not abused but also has the consequence of enhancing the reputation of the police as a fair-dealing body. It is the very values that underlie police governance that ensure it. In order to illustrate the relevance of the study of ethics, the use of authority in the criminal justice system, a number of specific codes of ethics, ethical problems and issues that might arise for professionals in the criminal justice system are set out in the following sections. These problems and issues might, for example, be concerned with how to exercise authority, with how to deal with conflicts between the personal and the professional, or with ethical issues confined within one particular part of the system, such as juvenile justice.

2.0 Objectives

The focus of this unit is to examine code of ethics and the use of authority as ethical issues in criminal system.

3.0 Main body

A priori, it may be considered that questions of professional ethics would be of greater concern to members of the liberal professions than to public servants such as the police. However, professional ethics can also be important in the police profession, by its very nature and the conditions in which its members fulfil their function. A police officer has extensive powers conferred on him, and he exercises these powers in the context of professional duties, hence the necessity of an internalised ethic, which would certainly gain from a codification. Through such a code of professional ethics, the legal provisions normally contained in the general regulations for public servants are raised to the level of professional moral imperative. The code of professional ethics is then seen as a means of transmitting a standard, the purpose of which would be to induce police officers to adhere to a system of values combining professional efficiency with respect for basic liberties.

PRIMARY RESPONSIBILITIES OF A POLICE OFFICER

A police officer acts as an official representative of government who is required and trusted to work within the law. The Officer’s powers and duties are conferred by statute. The fundamental duties of a police officer include serving the community; safeguarding lives and property; protecting the innocent; keeping the peace; and ensuring the rights of all to liberty, equality and justice.

PERFORMANCE OF THE DUITES OF A POLICE OFFICER

A police officer shall perform all duties impartially, without favor or affection or ill will and without regard to status, sex, race, religion, political belief or aspiration. All citizens will be treated equally with courtesy, consideration and

dignity. Officers will never allow personal feelings, animosities or friendships to influence official conduct. Laws will be enforced appropriately and courteously and, in carrying out their responsibilities, officers will strive to obtain maximum cooperation from the public. They will conduct themselves in appearance and deportment in such a manner as to inspire confidence and respect for the position of public trust they hold.

DISCRETION

A police officer will use responsibility the discretion vested in the position and exercise it within the law. The principle of reasonableness will guide the officer's determinations and the officer will consider all surrounding circumstances in determining whether any legal action shall be taken.

Consistent and appropriate use of discretion, based on professional policing competence, will do much to preserve good relationships and retain the confidence of the public. There can be difficulty in choosing between conflicting courses of action. It is important to remember that a timely word of advice rather that arrest – which may be correct in appropriate circumstances – can be a more effective means of achieving a desired end.

USE OF FORCE

A police officer will never employ unnecessary force or violence and will use only such force in the discharge of duty as in reasonable in all circumstances. Force should be used only with the greatest restraint and only after discussion, negotiation and persuasion have been found to be inappropriate of ineffective. While the use of force is occasionally unavoidable, every police officer will only use the minimal level of force that is necessary and never engage in cruel, degrading or inhuman treatment of any person.

CONFIDENTIALITY

Whatever a police officer sees, hears or learns of, which is of a confidential nature, will be kept secret unless the performance of duty or legal provision requires otherwise. Members of the public have a right to security and privacy, and information obtained about them must not be improperly divulged.

INTEGRITY

A police officer will not engage in acts of corruption or bribery, nor will an officer condone such acts by other police officers. The public demands that the integrity of police officers be above reproach. Police officers must, therefore, avoid any conduct that might compromise integrity and thus undercut the public confidence in a law enforcement agency. Officers will refuse to accept any gifts, presents, subscription, favours, gratuities or promises that could be interpreted as seeking to cause the officer to refrain from performing official responsibilities honestly and within the law. Police officers must not receive private or special advantage from their official status. Respect from the public cannot be bought; it can only be earned and cultivated.

COOPERATION WITH OTHER OFFICERS AND AGENCIES
Police officers will be responsible for their own standard of professional performance and will take every reasonable opportunity to enhance and improve their level of knowledge and competence. An officer or agency may be one among many organizations that may provide law enforcement services to a jurisdiction. It is imperative that a police officer assist colleagues fully and completely with respect and consideration at all times.

PERSONAL/PROFESSIONAL CAPABILITIES
Police officer will be responsible for their own standard of professional performance and will take every reasonable opportunity to enhance and improve their level of knowledge and competence. Through study and experience, a police officer can acquire the high level of knowledge and competence that is essential for the efficient and effective performance of duty. The acquisition of knowledge is a never-ending process of personal and professional development that should be pursued constantly.

PRIVATE LIFE
Police officers will behave in a manner that does not bring discredit to their agencies of themselves. A police officer's character and conduct while off duty must always be exemplary, thus maintaining a position of respect in the community in which he or she lives and serves. The officer's personal behaviour must be beyond reproach.

Ethical Problems in the Use of Authority

• The use of authority to promote personal values
• The use of authority to avoid accountability for wrongdoing

Ethical Problems in the Relationship Between Personal and Professional Interests

- Using professional status to promote personal interests (religious, philosophical, financial, etc.)
- Using institutional time and materials for personal gain unrelated to legitimate work activity
- Engaging in or promoting professional activities that are contrary to personal values
- Engaging in public or private personal activity that is contrary to professional values (use of drugs, driving under the influence of alcohol, etc.)

Ethical Problems in Personal and Professional Commitments to Clients

- Behaving unethically in personal relationships with clients

- Using relationships with clients/public for personal gain (to acquire goods more cheaply, have work done for personal benefit, accepting gifts, etc.)

Ethical Issues in Criminal Justice and Public Policy

- The "War on Drugs"
- Government policies having implications for criminal justice professionals in issues such as youth confinement, fingerprinting of juveniles, and compulsory treatment such as mandatory participation in substance abuse programs or anger management
- Capital punishment
- The move away from rehabilitative juvenile justice policies toward more punitive policies
- Policies involving harsher penalties resulting in "prisoner warehousing"
- Government-imposed mandatory sentencing (three-strikes legislation, mandatory minimum sentences)
- Truth in sentencing policies
- Increased surveillance of citizens in society

Ethical Issues Resulting From Policing Policies

- Policing policy in domestic violence cases
- Police profiling
- Use of force
- Use of police discretion

Ethical Problems in Information Sharing

- The ethics of withholding information; for example, from a client, the court, or the police
- Problems of confidentiality and privileged communication; for example, counsellor/ client relationships and participation in research
- Rules or practices relating to the retention or disposal of court records; for example, in the juvenile system where some states are now considering making juvenile records and court hearings open to the public and the media

Ethical Problems Dealing With Human Rights Issues in the Criminal Justice System

• The administration of cruel and unusual punishment

• Human rights violations against prisoners (women, men, juveniles)

• Capital punishment

Ethical Issues in the Media Reporting of Crime

• Crime and public opinion
• Crime as entertainment
• The politicization of crime

Self Assessment Exercise
Succinctly highlight and discuss five ethical issues in law enforcement

4.0 Conclusion

There are many issues facing today's police officer and other law enforcement agencies. Some include the police use of excessive force, deadly force, police corruption, police pursuits and other popular police related topics. Irrespective of these there are code of ethics guiding the profession. All police agencies throughout the country should be required to adopt the code of ethics as part of their policies and procedures. Each department should make it mandatory for officers to know as a matter of training what the code of ethics document represents. The departments should hold annual ceremonies were officers renew their code of ethics and oath of office.

5.0 Summary

This session concludes major discussions from previous units with emphasis on ethics and all related subjects. Most import of all is the role of ethics in shaping decisions in the profession of law enforcement. Ethics has been shown to be a central component in decisions involving ethical dilemmas, and the process of analyzing an ethical dilemma has been illustrated. Ethics is concerned with standards of conduct and with “how I ought to act,” and standards of conduct may vary among different societies. Approaches to setting standards range from cultural relativism to moral absolutism; a perspective that emphasizes moral pluralism seems to offer the best hope for resolving problems of relativities. Investigating sources of ethical standards reveals that religion, natural law, and other forms of law have an influence in shaping ethical standards. An understanding of ethics is essential to competent decision making by criminal justice professionals and to the proper working of the criminal justice system. Specifically, this unit show cases the importance of codes of professional ethics in law enforcement.

.

6.0 Tutor Marked Assignment

What are the Advantages of professional codes of conduct for the police?

7.0 References/ Further Reading

Arrington, R. 1983. "A Defence of Ethical Relativism." *Metaphilosophy* 14: 225–239.

Bunting, Harry. 1996. "A Single True Morality? The Challenge of Relativism." Pp. 73–85 in *Philosophy and Pluralism*, edited by David Archard. Cambridge: Cambridge University Press.

Cook, John. 1999. *Morality and Cultural Differences.* New York: Oxford University Press.

Death Watch. 2002. "New Orleans: Recent History 1996." Retrieved January 28, 2002 (www. hrw.org/reports98/police/uspo93.htm).

Felkenes, G. 1987. "Ethics in the Graduate Criminal Justice Curriculum." *Teaching Philosophy* 10(1): 23–26.

Glover, Jonathan. 1999. "Capital Punishment." Pp. 245–253 in *The Right Thing to Do: Basic Readings in Moral Philosophy* (2nd ed.), edited by J. Rachels. Boston: McGraw-Hill.

Hare, R. M. 1987. "Moral Conflicts." Pp. 205–238 in *Moral Dilemmas*, edited by C. Gowans. New York: Oxford University Press.

Hinman, L. 1998. *Ethics: A Pluralistic Approach to Moral Theory.* Fort Worth, TX: Harcourt

Brace. Holmes, Robert. 1998. *Basic Moral Philosophy* (4th ed.). Belmont, CA: Wadsworth.

Kane, R. 1996. *Through the Moral Maze: Searching for Absolute Values in a Pluralistic World.* Armonk, NY: North Castle Books.

Ladd, John. 1973. *Ethical Relativism.* Belmont, CA: Wadsworth. "92nd death row inmate freed since '73: Louisiana." January 5, 2001. *New York*

Times. Retrieved January 2002 (www.truthinjustice. org/no92.htm).

Rachels, J. 1991. "Subjectivism." Pp. 432–441 in *A Companion to Ethics*, edited by P. Singers. Cambridge, MA: Blackwell Press.

Singer, Peter. 1995. *How Are We to Live? Ethics in an Age of Self-Interest.* Amherst, NY: Prometheus Books.

Womack, Mari. 1995. "Studying Up and the Issue of Cultural Relativism." *NAPA Bulletin* 16: 48.

UNIT 6
Law Enforcement Agencies and Taser Usage

1.0 Introduction

The use of tasers by law enforcement agencies in general, and by police officers in particular, has become one of the most controversial issues in the area of criminal justice policy. This is in part because the issues are at the same time extremely straightforward (in that the only real question is the extent to which the use of tasers is and should be authorized) and uncomfortably complex (in that this question is by no means an easy one to answer).There are a number of premises upon which all interested parties should be able to agree. First, it is preferable to incapacitate a violent individual than to kill that individual. Second, the use of tasers should be permitted to the extent that such use is necessary to protect officer safety while minimizing the risk of physical

injury to suspects. Third, police officers should have some understanding of the effects that using a weapon is likely to have upon a suspect before deploying the weapon in question. Unfortunately, however, agreeing on the validity of these premises does not lead anyone to any obvious conclusions regarding the legitimate use of tasers by police officers.

2.0 Objectives

This unit is directed solely to the question of when, and under what circumstances, police officers should be authorized (and perhaps required) to use a taser on a suspect.

3.0 Main body

3.1 THE EFFECTS OF TASER USE ON THE HUMAN BODY

The vast majority of tasers purchased and used by law enforcement agencies are manufactured by Taser International (www.taser.com), which makes essentially two models of tasers, the M26 and the X26. Both models can be used in one of two modes, which produce different effects on the body. When used in firing mode, both the M26 and the X26 fire two probes up to a distance of 21 feet. They are programmed to deploy five-second bursts of electricity, although the charge can be prolonged indefinitely if the operator's finger remains on the trigger. The probes are attached to copper wires, which remain connected to the weapon. The shock can be repeated countless times, so long as both probes remain attached to the subject. Both models contain a cartridge of compressed nitrogen that fire the probes, and which must be reloaded every time the officer wants to fire. Both models have laser sights for accurate targeting and a built-in memory to record the time and date of each firing. Both models operate on 26 watts of electric output. Both deliver a 50,000-volt shock, which is designed to override the subject's central nervous system, causing uncontrollable contraction of the muscle tissue and instant collapse. The primary difference between the two models appears to be in design (the X26 is 60% smaller than the M26), although Taser International reports that the X26 has an incapacitating effect that is 5% greater than the M26. When used in "drive-stun" mode (at point blank range), the taser attacks the sensory nervous system. Rather than causing a complete override of the central nervous system, the weapon is essentially used as a pain-compliance technique. In this mode, the taser is used without the air cartridge. It applies shocks directly to the subject's body, skin, or clothing. The duration is the same as when the taser is used in firing mode (five seconds unless the officer keeps his hand on the trigger for longer). The clear consensus of the research is that a one-time five-second shock does not seriously or permanently injure a healthy and sober young adult who is not pregnant. However, the few studies that have been conducted, as well as the anecdotal evidence, suggest that there are some serious health risks involved when individuals not falling within that category are tasered.

Taser International includes the following product warnings on its website:

1. The TASER device can cause strong muscle contractions that may cause physical exertion or athletic-type injuries to some people. These muscle contractions can result in strain-type injuries such as hernias, ruptures, or other injuries to soft tissue, organs, muscles, tendons, ligaments, nerves, joints, and stress/compression fractures to bones, including vertebrae. People with pre-existing injuries or conditions such as osteoporosis, osteopenia, spinal injuries, diverticulitis, or previous muscle, disc, ligament, or tendon damage may be more susceptible to these types of injuries.

2. These strong muscle contractions usually render a subject temporarily unable to control his or her movements and may result in secondary injuries. Under certain circumstances, this loss of control can elevate the risk(s) of serious injury or death. These circumstances may include, but are not limited to, use of the TASER device on a person who is physically infirm or pregnant, or a person on an elevated or unstable platform, operating a vehicle or machinery, running or in water where the inability to move may result in drowning.

3. When practicable, avoid prolonged or continuous exposure(s) to the TASER device electrical discharge. The stress and exertion of extensive repeated, prolonged, or continuous application(s) of the TASER device may contribute to cumulative exhaustion, stress, and associated medical risk(s). Severe exhaustion and/or over-exertion from physical struggle, drug intoxication, use of restraint devices, etc. may result in serious injury or death. The TASER device causes strong muscle contractions, usually rendering a subject temporarily unable to control his or her movements. Under certain circumstances, these contractions may impair a subject's ability to breathe. If a person's system is already compromised by overexertion, drug intoxication, stress, pre-existing medical or psychological condition(s), etc., any physical exertion, including the use of a TASER device, may have an additive effect in contributing to cumulative exhaustion, stress, cardiovascular conditions, and associated medical risk(s).

4. TASER probes can cause significant injury if deployed into sensitive areas of the body such as the eyes, throat, or genitals. If a TASER probe becomes embedded in an eye, it could result in permanent loss of vision. Repetitive electrical stimuli can induce seizures in some individuals.

5. In most areas of the body, wounds caused by TASER probes will be minor. TASER probes have small barbs.

6. Use of a TASER device in drive (or touch) stun mode can cause marks, friction abrasions, and/or scarring that may be permanent depending on individual susceptibilities or circumstances surrounding TASER device use and exposure.

There are several things worth noting about these warnings. First, in most instances, an officer will find it nearly impossible to anticipate whether a subject suffers from any of the conditions listed. For example, except where pregnancy is fairly advanced, an officer is not likely to know a woman is pregnant. No officer would likely be able to discern that an individual suffers from a pre-existing injury or condition such as osteoporosis, osteopenia,, spinal injuries, diverticulitis, or previous muscle, disc, ligament, or tendon damage. An officer is unlikely to know whether a subject suffers from a respiratory impairment such as asthma, or from a pre-existing cardiovascular condition. Moreover, with respect to pregnancy, Taser International warns against use of a taser on a pregnant woman because of the risk that she would suffer from involuntary muscle contractions, thereby increasing the risk that she will fall and damage the fetus. The warnings listed above do not include any mention of risk to the fetus of the electrical shock itself. Nevertheless, there have been cases in which women have miscarried after being tasered. In the City of Chula Vista, Cindy Grippi was six-months pregnant when she was tasered and she miscarried twelve hours after being shot. The autopsy report did not conclude that the electro-shock was the cause of death; nonetheless, some studies have suggested a link between electro-chock and miscarriage and the city was sufficiently concerned about these studies that it paid her $675,000 to settle her lawsuit.

There are three overarching scenarios that cause concern regarding the possibility of a taser delivering a fatal shock. One is the possibility that a shock could occur during the “vulnerable period” of a heart beat cycle. Essentially, this means that there is a section of a heart beat cycle (specifically, three percent of the cycle) during which an electro-shock is highly likely to cause ventricular fibrillation, “a state in which the heart muscles spasm uncontrollably, disrupting the heart’s pumping function and causing death.” Second, certain individuals, such as children, the elderly, people with pre-existing cardiovascular problems, drug users, and individuals who take certain psychiatric medications, are naturally more susceptible to ventricular fibrillation than healthy young adults. Third, multiple and/or prolonged applications of a taser can increase the risk of cardiac arrest either by simply increasing the chances that a charge will shock the heart during the vulnerable period or by increasing the level of acid in the blood, which, in turn, decreases respiration and increases the risk of ventricular fibrillation.

Finally, there have been several reported fatalities in the state of California that have involved the use of tasers, most often in cases in which the subject was under the influence of drugs. Andrew Washington died in Vallejo in September

2004 after being tasered seventeen times. The cause of death was reported as "cardiac arrest associated with excitement during the police chase and cocaine and alcohol intoxication, occurring shortly after Tasering." Gregory Saulsbury died in Pacifica in January 2005, after being tasered eleven times. He had been using cocaine. Carlos Casillas Fernandez died in Santa Rosa in July 2005 after being tasered six times. He had been using methamphetamine. In sum, tasers pose some grave risks that warrant significant research and study. Not enough is known about the risks of taser use to children, the elderly, pregnant women, or those under the influence of drugs. From what little scientific research exists, it appears that prolonged and/or multiple use of a taser dramatically increases the risk of ventricular fibrillation and consequent cardiac arrest, even in healthy adults. In addition, there appears to be a risk of vision impairment if a subjected is tasered in the eye, and of seizure if a subject is tasered in the head. It is unclear whether there are medical risks associated with the barbs that are left in a subject's body once the probes are removed. There also appear to be permanent, if not fatal, dermatological impairments associated with the use of a taser in stun mode.

LEGAL ISSUES

Taser International has published a Memorandum of Law citing and purporting to explain the legal relevance of several state and federal court opinions. Presumably, in writing this memo Taser International intended to provide municipalities with arguments that they can raise in their defense of actions brought on behalf of individuals injured or killed by a taser. However, Taser International's legal analysis is substantially flawed, and we conclude that no municipality can safely rely on its conclusions to avoid liability in such an action.

The U.S. Court of Appeals for the Sixth Circuit made one of the earliest legal rulings addressing the use of tasers in 1992. In that case, *Russo v. City of Cincinnati*, members of the Thomas Bubenhofer estate sued the city of Cincinnati after Mr. Bubenhofer was shot to death by Cincinnati police officers. Mr. Bubenhofer had shut himself up in his apartment after being released by his mental health facility on a day pass and the family contacted the police. When the police arrived, Mr. Bubenhofer, a diagnosed paranoid schizophrenic, was in the apartment armed with two knives. Several times he approached officers, threatening them with the knives. Mr. Bubenhofer was eventually shot with both a taser and a firearm and subsequently died. The Sixth Circuit eventually held that the officers were entitled to "qualified immunity" and ruled that all the claims must be dismissed. Taser International hails this as a major victory for proponents of Taser use. But there is little legal basis for such a view, for several reasons. First, in 1992, the Department of Alcohol, Tobacco, and Firearms classified tasers as firearms. Therefore, the court was looking at the plaintiff's claims as a matter of the justifiable use of firearms in general. The ATF no longer classifies tasers as firearms, so it is not clear how, if at all, the case would apply to the use of tasers. Second, the court

did not hold that the use of the taser was justified, required, harmless, or permissible. Rather, in granting qualified immunity, the court simply held that the officer who fired the taser could not be held liable because the use of the taser did not violate clearly established law because there simply was no clearly established law regarding taser use at the time the officer fired one.

In sum, *Russo* does not in any way protect police officers from liability for injuries caused by use of a taser. Taser International also cites *Ewolski v. City of Brunswick* as legal support for the liberal use of tasers by police officers. In its memo, Taser International states that the court "held that the defendant police officer's use of Taser non-lethal force to subdue a potentially homicidal individual did not transgress clearly established law" and that the court "further held that the use of Taser non-lethal force against an armed and volatile suspect does not constitute excessive force and concluded that the defendant police officers are entitled to qualified immunity on the Plaintiff's excessive use of force claim." These statements are at best misleading and at worst entirely false. The officers involved in the *Ewolski* case did not even use tasers. In that case, the court held that the officers in question were entitled to qualified immunity for their use of a battering ram and tear gas in a hostage situation involving a man who had been threatening to shoot any officer who entered his home and who had, in fact, already shot one officer. The court does quote language from the *Russo* case addressing the standard to be applied in evaluating a defense of qualified immunity. However, to state that the court upheld *Russo* and concluded that a use of a taser was justified is a mischaracterization of both the facts of the case and the relevance of its legal conclusions. No municipality should rely on Taser International's analysis of this case in defending an excessive force claim regarding the use of tasers. The other cases addressed by Taser International are *Lifton v. City of Vacaville*, 2003 U.S. App. LEXIS 16286 (9th Cir. 2003), *Michenfelder v. Sumner*, 860 F.2d 328 (9th Cir. 1988), *Jolivet v. Cook*, 1995 U.S. App. LEXIS 3950 (10th Cir. 1995), *Walker v. Sumner*, 1993 U.S. App. LEXIS 26517 (9th Cir. 1993), *Caldwell v. Moore*, 968 F.2d 595 (6th Cir. 1992), *Hernandez v. Terhume*, 2000 U.S. Dist. LEXIS 18080 (N.D. Cal. 2000), *Hinton v. City of Elwood*, *Drummer v. Luttrell*, 75 F.Supp.2d 796 (W.D. Tenn. 1999), *Bennett v. Cambra*, 1997 U.S. Dist. LEXIS 1584 (N.D. Cal. 1997), *Alford v. Osei-Kwasi*, 203 Ga. App. 716 (1992), *Nicholson v. Kent County Sheriff's Dep't*, 839 F.Supp. 508 (W.D. Mich. 1993), and *Parker v. Asher*, 701 F.Supp. 192 (Nev. 1988). No municipality can safely rely on Taser International's analysis of these cases in defending an excessive force claim regarding the use of tasers. *Lifton* is unpublished and, therefore, not binding. In its opinion, the court does not set out any of the underlying facts; therefore, the case provides no guidance on when and under what circumstances the Ninth Circuit Court of Appeals would consider use of a taser acceptable. *Michenfelder* was a 1998 case raising an Eighth Amendment challenge to prison guards' use of a taser to compel inmate strip searches and is therefore inapplicable to the questions presented within the context of this report. *Jolivet* is an unpublished (and, therefore, not binding)

case holding that the use of a taser in a prison did not violate the Eighth Amendment. *Caldwell v. Moore* is a 1992 case holding that the use of a taser in a prison did not violate the Eighth Amendment because the use was not "maliciously and sadistically to cause harm." *Hernandez* and *Bennett* are both unpublished federal district court cases that address Eighth Amendment challenges to the use of tasers in the prison context. The company's citation to *Hinton* is errorenous, since the case cannot be located in the Westlaw database. *Drummer* did not even involve a taser; the federal district court merely cited *Caldwell v. Moore* for the proposition that the use of a taser in a prison may, under certain circumstances, not violate the Eighth Amendment. The remaining cases are similarly unhelpful in guiding a municipality in developing guidelines for the appropriate use of tasers by law enforcement officers. The City of Mountain View should also be aware that several municipalities have paid substantial amounts to settle excessive force actions brought by individuals who were injured by police use of tasers. The city of Chula Vista, California, paid $675,000 to settle a claim brought by a woman who lost her baby after being shot by a taser. The officer involved had tasered the woman in the back, as she was attempting to enter her house. She had not been engaged in criminal activity and was not armed. The city of Portland, Oregon, paid $145,000 to settle an action brought by a 71-year-old woman who had been tasered. The woman had refused to obey orders that she not enter a trailer, so the officers involved hit her in the head with a taser, knocking her to the ground, and then shot her three times with the taser.

***A note on international standards*:** This report focuses on American (federal and state) legal rules that might apply to tasers. But we also we note that tasers have also received attention from the perspective of broader human rights commentary, as guided by international law or convention. Amnesty International has stated that that there are three over-arching human rights issues associated with police use of tasers. One is that because tasers are portable and easy to use, they are particularly open to abuse by unscrupulous officers. The second is that police officers appear to be using tasers as a routine force option, rather than as an alternative to lethal force (there are numerous incidents in which tasers have been used to subdue people who aren't posing a serious danger to officers, against unruly schoolchildren, on unarmed mentally ill and intoxicated people, and on suspects fleeing minor crime scenes or failing to comply immediately with commands). The third is that there appears to be a growing number of fatalities associated with police use of tasers. Amnesty International states that the inappropriate use of tasers may violate the United Nations Code of Conduct for Law Enforcement Officers, the Basic Principles on the Use of Force by Law Enforcement Officials, and the United Nations Convention on the Rights of the Child. It should be noted that only a small number of specially trained officers are permitted to carry tasers, and are permitted to use them only under circumstances in which use of a firearm would also be permitted. Additional information regarding the applicability of

international human rights law to the use of tasers can be found at RECOMMENDATIONS

1. The Use of Tasers by Police Officers should be limited to circumstances under which the use of lethal force would also be permitted.

First, here is a snapshot of the established law on the authorized use of force by police: Police can always use reasonable, non-deadly force to thwart any crime or to seize anyone the police officer reasonably believes to be fleeing from the commission of a crime or attempting to evade a lawful arrest. As for deadly or "lethal" force – usually defined to mean force intended to or likely to cause either death or grievous bodily harm – police can use this to *prevent* completion or commission of a felony only if the felony is one that normally poses serious physical danger to victims or bystanders (robbery, rape) but not for other, non-violent felonies. In addition, under the Supreme Court rules established in *Tennessee v. Garner*, 471 U.S. 1 (1985), police may only use deadly force to *apprehend* or to ensure the arrest of someone fleeing from the commission of a felony if the office reasonably believes that the fleeing person at the time of flight poses a threat of death or serious bodily injury to others.

We recommend that all countries adopt a specific policy limiting police use of tasers to situations in which they would also be permitted to use deadly or lethal force. Because the health effects of tasers have not been adequately studied, we contend that the use of a taser in any other situation would constitute excessive force. Courts that have been confronted with this question have tended to hold that police officers who injure or kill suspects with a taser are entitled to qualified immunity. As more becomes known regarding the health effects of tasers, however, this may change. Moreover, the availability of qualified immunity holdings does not protect a city from being in the unfortunate position of having to settle a lawsuit brought by a citizen who has been severely injured by the police use of a taser. For these reasons, tasers should be considered as a lethal force option on the use of force continuum. We also recommend, consistent with the above, that police officers be encouraged to use tasers as an alternative to lethal force. Tasers should be the preferred method of use of force in life-threatening situations, and should not be used otherwise. This recommendation represents a cautious assessment of the costs and benefits of taser use. Assuming that tasers are efficacious in constraining people from committing or fleeing crimes, tasers are no less beneficial to police than are firearms. They are less costly to society in that they will prevent the death or grievous injury that would occur were firearms used in deadly force situations where something else than death or grievous injury would be sufficient to achieve the police purpose. Tasers may also be more beneficial to law enforcement in two senses: First, since some feeling felons try to seize the guns of police officers and use the guns against the officers or other innocent people, that risk is reduced if the officer does not take out a gun against the felon. Second, assuming that within the gray legal zone of permissible use of deadly force some police officers will be understandably

conservative in deciding whether to shoot, they will be more effective in thwarting or capturing felons if they are more comfortable in using tasers than guns. Two alternative positions are conceivable. First, once could take a less cautious view of the current research and conclude that taser use does not pose much risk, if any, of death or grievous bodily harm, and therefore should not be treated as "deadly force" under the law. We think it very unwise to read the current research that way. Second, one could argue that because tasers, even if sometimes lethal, surely cause death or grievous bodily injury *less often* than do guns, the police ought to be authorized to use them even in situations where deadly force is not authorized. We believe that given the current uncertainty about the measurable risk of death or grievous injury posed by tasers, and given the difficulty, if not impossibility, of police officers on the street discerning whether the target is an especially vulnerable victim, this is an unwise and unworkable legal position.

2. Training

Taser International provides training materials to law enforcement agencies and at least fifty-two law enforcement agencies in the state of California use them as their sole source of training. At least four agencies in the state of California create and use their own training materials. This is inappropriate. The city of Mountain View should solicit assistance and information from law enforcement agencies that have developed their own materials and *not* rely on those provided by Taser International. Taser International's training materials downplay the risks associated with taser use, encourage multiple firings in inappropriate circumstances, and misrepresent the studies that have been done regarding the health effects of tasers. The city of Mountain View should also require its law enforcement agencies to follow the recommendations and training protocols set forth by the International Association of Chiefs of Police. This is a nine-step policy and training protocol that the IACP developed in response to concerns raised by the law enforcement community about the use of tasers. The recommendations are generally sound and are in accord with established legal and civil rights principles.

3. Tasers should NEVER be used under certain circumstances

There has not been sufficient independent testing on the safety of tasers on vulnerable populations such as children, pregnant women, the elderly, the mentally ill, and those under the influence of drugs. Therefore, the city of Mountain View should strongly consider adopting a policy prohibiting the knowing use of tasers on such individuals. Clearly, a police officer may not know whether a woman is pregnant or whether any particular individual is taking psychiatric medications. Therefore, such a policy need not punish officers who inadvertently injure a suspect whom he or she did not know was a member of such a vulnerable population. Nonetheless, a sound policy would advise police officers that the use of tasers on such individuals may be extremely dangerous and that knowingly using a taser on such an individual is never appropriate. The purpose of tasers and other weapons is to subdue violent

and dangerous individuals. Therefore, the city should adopt a policy prohibiting the use of tasers for the purpose of inflicting punishment or pain. Tasers should be used only on dangerous individuals and never on individuals who are passively resisting arrest.

Self Assessment Exercise

1. **What is Taser? What are the ....to guide against when using a it?**
2. What are the advantages as well as the disadvantages in the usage of taser?

4.0 Conclusion

The use of tasers by law enforcement officers is almost entirely unregulated. Therefore, any municipality or state that endeavors to implement a policy guiding law enforcement agencies in the appropriate use of tasers should be commended.

5.0 Summary

The first section of this unit gives a brief summary of the effects of taser use on the human body. The second section provided a summary and analysis of the legal issues that have arisen in connection with the use of tasers, and of the existing case law that addresses these legal issues. The final section offer some guidance regarding the possible appropriate uses of tasers and some recommendations.

4. Recommendations

The San Jose Police Department requires officers to transport subjects hit with taser barbs to a hospital so that medical personnel can remove the barbs. Many agencies call EMTs to the scene of a taser use so that they can monitor the subject and remove the barbs if doing so is appropriate. Mountain View should establish a specific policy on this issue requiring the intervention of some type of medical personnel. Permitting officers to remove the barbs is inappropriate. Police officers should be required to document every use of a taser, including situations in which a taser is shown or threatened, even if not used. The documentation should include identifying information regarding the subject such as age, race, physical health, degree of intoxication if any, and medications taken if any. The documentation should also include information regarding the circumstances of the taser use itself, including the actions of the subject, the basis for the use of the taser, whether the individual was arrested, the number of times the taser was used, and whether it was used in stun gun mode or shot from a distance. Collecting such information can only assist municipalities in developing and revising guidelines regarding taser use.

6.0 Tutor Marked Assignment

Explain the three overarching scenarios that can cause concern regarding the possibility of a taser delivering a fatal shock.

7.0 References/ Further Reading

IACP Report. http://www.iacp.org/research/CuttingEdge/EMDT9Steps.pdf.
http://www.cpoa.org/forcechart.html for a visual representation of the use of force continuum
generally followed by law enforcement agencies. See GAO Report for more information on this issue generally.

http://www.amnestyusa.org/countries/usa/document.do?id=1A01E91E134A327080256F190042408D. Amnesty International, "Excessive and Lethal Force? Amnesty International's Concerns.

Deaths and Ill-treatment Involving Police Use of Tasers," Vol. 1(7).
http://www.amnestyusa.org/countries/usa/document.do?id=1A01E91E134A327080256F190042408D
http://www.taser.com/law/download/memo.htm. (Taser Memo).

ACLU of Northern California, "Stun Gun Fallacy: How the Lack of Taser Regulation Endangers Lives," September 2005 ("ACLU Report"), p. 4, citing Russel Sabin, "Heart Expert Warns About Using Tasers," San Francisco Chronicle, January 5, 2005.
Taser International website, Product Warnings for Law Enforcement. www.taser.com/safety/.
Warnings 6-12. Note, the warnings given to civilian taser owners differ slightly from the warnings given

UNIT 7
Intelligence Agencies Support and Law Enforcement

1.0 Introduction

The collapse of the Soviet Union and the Warsaw Pact by 1991 significantly altered the international environment. Transnational issues, such as narcotics, terrorism, money laundering, economic espionage, and shipments of materials for weapons of mass destruction (WMD) have risen in importance, in some cases becoming more urgent than traditional geopolitical concerns. In seeking to take action against such criminal activities occurring in foreign countries, it has seemed logical to many to bring to bear the enormous information gathering capabilities of the Intelligence Community which has both collection systems and human agents available throughout the world. It would, some have argued, be relatively simple to make information obtained by intelligence agencies available to investigators and prosecutors in support of the latter' efforts to bring terrorists and narcotics traffickers to justice in courts. Some observers would, of course, go further, suggesting that, in especially threatening cases, covert actions by the CIA or military strikes might be necessary.

2.0 Objectives

This unit aims at examining the processing of security information by intelligence agencies and investigators.

3.0 Main body

Closely coordinating the efforts of law enforcement agencies and the Intelligence Community (alongside the State and Defense Departments) presents, however, significant challenges. As three knowledgeable observers have written:

> The law enforcement/national security divide is especially significant, carved deeply into the topography of American government. The national security paradigm fosters aggressive, active intelligence gathering. It anticipates the threat before it arises and plans preventive action against suspected

> targets. In contrast, the law enforcement paradigm fosters reactions to information provided voluntarily, uses ex post facto arrests and trials governed by rules of evidence, and protects the rights of citizens.

The division of responsibilities between intelligence and law enforcement agencies reflects this reality and is based in statutes and executive orders. Many observers—including intelligence agency officials—strongly believe in the fundamental importance of distinctions between law enforcement efforts, governed by laws and rules designed to protect the rights of the accused, and the far less restricted operations of intelligence agencies. The National Security Act of 1947, that established the CIA, specifically precluded the Agency from having any responsibilities for law enforcement or internal security. This provision derived from a determination shared by Congress and the Truman Administration not to create an American "Gestapo" or to encroach on the jurisdiction of the FBI. There was then, as there remains today, a concern that "combining domestic and foreign intelligence functions creates the possibility that domestic law enforcement will be infected by the secrecy, deception, and ruthlessness that international espionage requires." The 1947 Act also reflected the division of labor during World War II between the Office of Strategic Services (OSS), the CIA's predecessor intelligence service, and the FBI (even though the latter undertook extensive intelligence gathering in Latin America). Most of the other elements of the U.S. Intelligence Community are located in the Department of Defense (DOD), which also has been largely precluded from direct involvement in domestic law enforcement efforts since the post-Civil War enactment of the *Posse Comitatus* statutes. DOD has received legal authority to assist law enforcement agencies in counternarcotics efforts, although with restrictions precluding any involvement of military personnel in the arrest and detention of uspects.

In some cases, efforts of intelligence agencies in support of law enforcement efforts proved to be ill-advised. In particular, instances of intelligence agencies acquiring information concerning U.S. citizens or persons have been widely condemned. In addition to various questionable Cold War activities, such as mail openings and involvement with the Mafia, the CIA and military intelligence units gathered intelligence on antiwar groups within the United States during the Vietnam War period. Such activities served as a major impetus for wide-ranging congressional investigations of the U.S. Intelligence Community in the 94th Congress. In the aftermath of sensational revelations about improper activities by intelligence agencies, both the Intelligence Community and its congressional overseers were determined to separate the work of intelligence and law enforcement agencies in order to prevent the use of intelligence techniques against citizens and legal residents of the United States unless court orders have been obtained. Proposals for enacting a charter for the Intelligence Community did not succeed, but the widespread criticisms of domestic spying by the CIA and other intelligence agencies served to build

walls of separation between the two communities that were widely recognized in practice even if cooperation on narcotics and terrorism was officially allowed. A study prepared by the House Intelligence Committee in 1996 concluded that, "One of the unwritten but significant side effects of these investigations was behavioral in nature. The years that followed the investigations were marked by some reluctance on the part of the two cultures to form interactive relationships. This over-caution was based more [on] a perception that closer association meant increased political risk than [upon] having any basis in prohibition of law." Even before the end of the Cold War, however, terrorism and narcotics smuggling were emerging as matters of national concern. Executive Order 12333, *United States Intelligence Activities*, signed by President Ronald Reagan on December 4, 1981, specifically assigned the CIA responsibilities for collecting and producing intelligence on foreign aspects of narcotics production. Intelligence agencies were authorized "to participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities ...."

With the end of the Cold War, intelligence agencies have had to adjust their efforts to meet changed national security requirements. By the mid-1990s they were downsized roughly by a third from 1980s levels and many Cold War missions disappeared. (Funding levels have risen somewhat more recently.) The Intelligence Community has faced major challenges in adjusting its expensive technical collection systems—satellites and signal intercept efforts—to the changed environment. It is now making much greater use of open sources, *i.e.* books, newspapers, radio and television programs, and pamphlets. Human collection has been a particular challenge inasmuch as the personnel and methodologies useful for collecting information about topics such as Soviet diplomatic or military policies are far different than those necessary to collect information about a terrorist or drug-smuggling group. The emergence of transnational threats in recent years and the availability of intelligence resources led many to urge greater use of Intelligence Community assets to obtain information that may, at some point, be used in criminal proceedings. The Intelligence Community collects a wealth of data about all regions of the world. Its data storage and retrieval capabilities, as well as thousands of trained analysts, could potentially be of enormous use in support of law enforcement efforts. In some parts of the world, intelligence contacts unique access can provide invaluable information concerning activities that may be related to violations of U.S. law. Although the vast bulk of intelligence collection is, and will likely remain, focused on topics far removed from the concerns of law enforcement agencies, the use of intelligence information has been seen as having important potential advantages with the increasing global scope of much criminal activity. Even as the Cold War was reaching its final stages, demands for closer intelligence and law enforcement cooperation intensified during the course of investigations of two international banking scandals during the late 1980s. There was considerable public consternation when it was

learned that the CIA had acquired information about potential wrongdoing that had not been readily made available to the Justice Department; intelligence information about the activities of the Bank of Credit and Commerce International (BCCI) and Banca Nazionale del Lavoro (BNL) was apparently shared with prosecutors in haphazard and uncoordinated ways; some never emerged outside the Intelligence Community. Although most observers did not conclude that there was an effort by CIA to protect either of these two banks, congressional committees recommended that procedures be established to ensure that relevant information about international criminal activity collected by intelligence agencies would be made available to law enforcement officials even though, in some cases, the need to protect sources and methods would undoubtedly make it impossible to use the information directly as evidence in a trial.

Law Enforcement Agencies Acquire International Missions

In responding to new expectations and a changed environment, the FBI has assigned increased numbers of agents abroad. In June 1996, the FBI launched a four year plan to double the number of FBI officials serving in legal attaché offices of U.S. embassies; additional positions have subsequently been authorized. Offices opened in recent years include Cairo, Egypt; Islamabad, Pakistan; Tel Aviv, Israel; Moscow; Tallinn, Estonia; Kiev, Ukraine; Warsaw, Poland; Almaty, Kazakhstan; Prague, Czech Republic; Tashkent, Uzbekistan; Pretoria, South Africa; New Delhi, India; and Buenos Aires, Argentina. Additional office are planned. The plan was expected to entail the assignment of a total of some 130 special agents and a lesser number of support staff. These offices are expected to serve a number of purposes. They permit the establishment of close “cop-to-cop” relationships by which law enforcement information can be exchanged with host-country officials. In addition, FBI officials are able to cultivate ties to other sources of information in the host countries. Then- FBI Director Louis Freeh has stated that the Legal Attaché program is “the single most significant factor in the Bureau’s ability to detect, deter, and investigate international crimes in which the United States or our citizens are victims.” Some observers have expressed concern that they would overlap or duplicate the work of CIA or other intelligence officials already assigned to these countries. Then-DCI John Deutch was reported to have had some initial reservations, but efforts were undertaken to work out cooperation arrangements.

In some countries, of course, rigid separation does not exist between intelligence and law enforcement agencies, and U.S. officials must carefully tailor their relationships with foreign counterparts. Inevitably, complications and overlap will arise, but they will, according to administration officials, be addressed on a case-by-case basis, with the ambassador or chief of station having a major role, consistent with that official’s statutory responsibility for “the direction, coordination, and supervision of all Government executive branch employees in that country.” Observers note that not all ambassadors

take an active interest in such concerns, that law enforcement and intelligence officials in embassies have not always been forthcoming with ambassadors, and that officials may be carrying out policies formulated by Washington agencies without the unqualified support of the State Department. Nonetheless, observers see disagreements, duplication of effort, or competition between FBI and intelligence officials in foreign countries as inevitable; potential problems which, while arguably outweighed by the benefits of "cop-to-cop" cooperation, will require careful monitoring.

Managing the Intelligence-Law Enforcement Relationship

In the aftermath of the wave of criticism and congressional direction that followed revelations of CIA's failure to provide information about the BCCI and BNL cases to Justice Department officials, a Joint Task Force on Intelligence and Law Enforcement was established in March 1993. The task force, chaired by Deputy Assistant Attorney General Mark Richard and CIA General Counsel Elizabeth Rindskopf, came up with a series of recommendations. Many of these proposals involved relatively technical and administrative efforts to improve information flow and data retrieval:

1. the creation of "focal points," *i.e.*, coordinating offices, in the Justice Department to interface with the CIA;
2. new procedures to govern requests for intelligence-file searches that might result in the production of materials to be used in court cases;
3. requirements for law enforcement agencies to provide notice to prosecutors when there is an intelligence interest;
4. measures concerning the treatment of the identity of intelligence officers whose identities are classified;
5. new procedures to protect classified information in situations not envisioned by earlier statutes, such as the Classified Information Procedures Act;
6. a Memorandum of Understanding between the Attorney General and intelligence agencies that outlines the circumstances under which the agencies must report suspected criminal activity; and,
7. an intercommunity training plan to facilitate coordination.

Although Deputy Assistant Attorney General Mark Richard claimed that "the problems between the CIA and Justice Department no longer exist," there remained, nonetheless, a realization that difficult substantive issues would continue to be involved in facilitating information flow. Rindskopf subsequently noted:

> There were three possible solutions: (i) to blend the two services and place them under rules governing the law enforcement community; (ii) to blend the two services and place them under intelligence rules; and (iii) to coordinate the activities of the two services. Ultimately, the decision was made to go forward with great caution.

A major challenge for promoting cooperation between intelligence and law enforcement agencies are their respective bureaucratic cultures, modes of operation, sources of information, and oversight structures. The Justice Department, which includes both the FBI and the DEA, is responsible for conducting investigations of possible law breaking, and prosecuting alleged criminals in the judicial system. Although law enforcement agencies need background information or "strategic intelligence" regarding patterns of criminal activity (*e.g.*, analysis indicating that increasing quantities of cocaine are flowing through harbours in southern Florida), they tend to give higher priority to tactical information (*e.g.*, a tip that a specific cargo vessel is scheduled to off-load a shipment of cocaine at a specific dock in Miami on the night of August 4). Under applicable rules of legal procedure, this latter type of information may have to be used in a public trial and its origins revealed to a defendant's lawyer. Law enforcement agencies typically work on a case-by-case basis; when a trial is completed and all appeals exhausted, the information developed in the preliminary investigation has little use and can be consigned to the archives.

However, national security policymakers require a continuous stream of information from the CIA and other intelligence agencies about world conditions, especially about countries, groups, and individuals working against U.S. interests. There is no end-point to these requirements; even a favourable evolution of events (such as the dissolution of the Soviet Union) does not mean the end of the need for up-to-date information. In many cases, the need for intelligence is more important than the need for dealing with a particular incident; thus, it may be advantageous to support a covert intelligence source for years (even if the source is publicly identified as anti-American or involved in illegal activities) and to keep the relationship with U.S. intelligence agencies secret. Public disclosure could not only destroy the source's usefulness, but also serve to undermine U.S. efforts to recruit and retain other sources. National security policymakers may, moreover, seek rumours and gossip that could never stand up in court. Such information may, nonetheless, provide the best indication of a fluid political situation in another country that could directly affect U.S. interests. Coordinative and consultative mechanisms—an Intelligence-Law Enforcement Policy Board and a Joint Intelligence-Law Enforcement Working Group (JICLE)—have been established at several levels in response to the 1994 assessment of the Joint Task Force on Intelligence and Law Enforcement reached to ensure that exchanges of information are soundly established and preserve the integrity of the judicial process, as well as the legitimate functions of the Intelligence Community. These entities have considered the nature and extent of appropriate law enforcement intelligence coordination in pre-trial discovery and established administrative policies regarding such cooperation. The Joint Task Force did not consider that a need existed for statutory changes. Concerns about the future of interagency relationships in the post-Cold War era were also reflected in the Intelligence

Authorization Act for FY 1995 (P.L. 103-359), signed on October 14, 1994. The Act established a commission to review the roles and capabilities of the Community. The resultant Commission on the Roles and Capabilities of the United States Intelligence Community made an extensive review of the activities of intelligence agencies, and concluded that:

> Law enforcement can be an extremely powerful weapon against terrorism, drug trafficking, and other global criminal activity. But it may not be the most appropriate response in all circumstances. Often the perpetrators have sought sanctuary in other countries and cannot be brought to trial. Compiling proof beyond a reasonable doubt—the standard in criminal cases—may be even more difficult with respect to global crime. Diplomatic, military, or intelligence measures, in many cases, can offer advantages over a strict law enforcement response, or can be undertaken concurrently with law enforcement.

The Aspin-Brown Commission recommended that direction of the effort be vested in a senior-level committee of the National Security Council (NSC), and that the committee include the Attorney General (who is not a member of the NSC). It urged the proposed committee to develop improved procedures to ensure increased sharing of information between the two communities, and to coordinate increasing law enforcement activities abroad with local U.S. ambassadors and with intelligence agencies. The Commission also noted the unwillingness of intelligence agencies to accept tasking from law enforcement agencies, based on their understanding that they were legally authorized to collect information for a valid foreign intelligence purpose.

Based on the need to maximize the effort against terrorism and other transnational threats, the Commission argued that "the Intelligence Community should be permitted to collect information overseas at the request of a law enforcement agency so long as a U.S. person is not the target of the collection or the subject of the potential prosecution." Intelligence agencies had long argued that, even if information could be shared with law enforcement agencies, it could be collected only for foreign intelligence purposes, law enforcement use being essentially a by-product. Based on the needs that had been perceived by the Aspin-Brown Commission to facilitate the intelligence contribution to the struggle against transnational threats, the FY1997 Intelligence Authorization Act (P.L. 104-293) (Section 814) amended the National Security Act to authorize elements of the Intelligence Community to collect information outside the United States about individuals who are not U.S. persons. They would do so at the request of law enforcement agencies, "notwithstanding that the law enforcement agencies intend to use the information collected for purposes of a law enforcement investigation or counterintelligence investigation." For the Defense Department, this

authorization extended only to NSA, the National Reconnaissance Office, and the National Imagery and Mapping Agency (and not to the intelligence offices of the military services). This seemingly minor shift was strongly criticized by some civil libertarians as a significant step towards a blurring of important distinctions between intelligence and law enforcement, and essentially giving NSA law enforcement responsibilities for the first time. In addition, Congress has undertaken to remove some statutory prohibitions that were seen as inhibiting intelligence support to law enforcement efforts. The Antiterrorism and Effective Death Penalty Act of 1996 (P.L. 104-132) included provisions that allow the use of "classified information" indicating terrorist connections in deportation hearings of aliens seeking entrance into the U.S. Presumably, the "classified information" could derive from either law enforcement or intelligence sources. The information need not be disclosed to the alien or his or her attorney beyond a summary "adequate to prepare a defense." Such use of classified information has been harshly criticized. Some observers, including some Members of Congress, believe that these provisions violate constitutional requirements for due process. Others, however, consider that revealing such information in deportation or visa cases could provide terrorist organizations with highly valuable information. In a widely reported case, former DCI James Woolsey, now an attorney in private practice, has challenged efforts of the Immigration and Naturalization Service to use classified materials to justify deportation of several Iraqis without sharing it with him as their counsel.

Another instance of intelligence and law enforcement cooperation is the National Drug Intelligence Center (NDIC) in Johnstown, Pennsylvania, which also reflects an effort to encourage law enforcement-intelligence cooperation in the counternarcotics effort. Established pursuant to the Defense Appropriation Act for FY1992 (P.L. 102- 172), NDIC includes personnel from both law enforcement and intelligence agencies. At its inception, it was expected that NDIC would make available information from both intelligence and law enforcement sources, enabling analysts to put together a comprehensive account of drug enterprises, identifying "the heart of a given organization, not just its extremities. Final success depends upon identifying and destroying those critical parts of the organization that are most vulnerable: key personnel, communications, transportation, finances, and essential supplies and equipment." NDIC's current mission is to coordinate and consolidate strategic organizational drug intelligence, and produce assessments of the structure, membership, finances, communication, transportation, logistics, and other activities of drug trafficking organizations. Although the extent of NDIC's success in fulfilling its mission has not been publicly detailed, Congress continues to provide funding. In recent years some $27 million has been authorized annually for NDIC with the Attorney General retaining full authority over NDIC's operations. The Conference Committee on the FY1999 Intelligence Authorization Act, in reiterating a request for a comprehensive assessment of the national counter-narcotics architecture, noted that: NDIC should be the facility that brings together all law enforcement and intelligence

information for integrated, all-source, cross-case analysis. The continued isolation of domestic and foreign aspects of the drug trafficking organizations for separate analysis by different intelligence centers ignores the transnational character of the drug trafficking threat to national security. Some observers continue to view NDIC is an organizational anomaly, managed by the Justice Department but with funding provided in intelligence authorization legislation. It represents a relatively small aspect of the much larger difficulty in addressing the law enforcement-intelligence relationship.

The FBI has been responsible for counterintelligence, protecting all U.S. government agencies from foreign penetration and for collecting information about threatening foreign activities in the United States. The CIA and FBI had longstanding arrangements for trading information on counterintelligence concerns, and CIA had established a Counterintelligence Center in 1986, but, according to many observers, there were limits to the extent of cooperation (as well as considerable ineptitude in both agencies) clearly reflected in the failure to identify and arrest Aldrich Ames in the nine years that he spied on behalf of the Soviet Union prior to his arrest in 1994. The Ames debacle made closer cooperation imperative. In a 1994 Presidential Decision Directive, a National Counterintelligence Policy Board was established by President Clinton and a separate National Counterintelligence Center (NACIC), located at CIA Headquarters, but not part of the CIA, was created to coordinate counterintelligence activities of various agencies. The staff of the NACIC are counterintelligence and security professionals detailed from the FBI, CIA, DOD, State, and the National Security Agency (NSA) and serving two year terms; the initial director was from the FBI, and successors will rotate from the FBI, CIA, and DOD for two year terms.

Observers perceived, however, that the NACIC lacked sufficiently high visibility to deal effectively with counterintelligence challenges. In January 2001, President Clinton signed a Presidential Decision Directive, U.S. Counterintelligence Effectiveness–Counterintelligence for the 21st Century" (CI-21), creating a National Counterintelligence Executive, reporting to the FBI Director and other senior officials, to coordinate a counterintelligence program. CI-21 will include strategic planning, analysis, counterintelligence budgeting, and information collection operations, serving as the national coordination mechanism to issue warnings of counterintelligence threats to the national security. The Office of the National Counterintelligence Executive became operational in May 2001. A Counterterrorist Center (CTC) was also established within CIA in 1986 to produce intelligence on terrorist threats. Although not a "national" center like the NACIC, the CTC now includes representatives from other intelligence agencies and from law enforcement and policy agencies as well. DCI Tenet has argued that the CTC:

> creates a whole that is greater than the sum of its parts. It harnesses all of the operational, analytical, and technical

> elements devoted to counterterrorism. The results through the years point to the soundness of this idea. The successes of this approach range from the uncovering of Libya's role in the bombing of Pan Am 103 to the thwarting of Ramzi Yousef's attempt to blow a dozen United States airliners out of the sky in the Far East during 1995. Moreover, CTC has worked with the State Department to provide extensive counterterrorist training to our allies. Over 18,000 individuals in 50 nations have been trained in counterterrorism over the past decade.

The capability to exchange information between intelligence and law enforcement agencies is widely considered essential, even if some observers continue to insist that "[i]ntelligence-gathering tolerates a degree of intrusiveness, harshness, and deceit that Americans do not want applied against themselves." Thus far, there has been a recognition that information acquired by intelligence agencies can be useful to law enforcement agencies, and procedures have been established to allow it to be transferred and used in ways that are intended not to compromise intelligence sources and methods, on one hand, or violate the constitutional rights of American citizens and persons, on the other. As cases are tried in the courts, the limits of the procedures will undoubtedly be tested, and the courts may limit or extend the permissibility of using information from the Intelligence Community. The extent to which "a bright red line" can be drawn is as yet uncertain. Important principles remain, however, that create limits to the extent of cooperation; the *Department of Justice Manual* (DOJM) states:

> Although coordination on matters of common concern is critical to the proper function of the two [*i.e.*, law enforcement and intelligence] communities, prosecutors must be aware of the concomitant need of both communities to maintain a well-delineated separation between criminal prosecutions and foreign intelligence activities, in which less-stringent restraints apply to the government. Not to do so may invite the perception of an attempt to avoid criminal law protections by disguising a criminal-investigation as an intelligence operation. The judicial response to that may be the suppression of evidence in the criminal case....

Above and beyond the interagency bodies comprised of members of law enforcement and intelligence agencies, White House-level entities have been established to provide government-wide coordination. The efforts of the Intelligence Community, as well as the State and Defense Departments, are coordinated by the National Security Council (NSC) staff under the direction of the President. Law enforcement actions are coordinated by the Attorney

General on behalf of the President. Concerns about executive branch oversight of the U.S. response to transnational threats led to the 1996 passage of amendments to the National Security Act of 1947. Section 804 of the FY1997 Intelligence Authorization Act (P.L. 104- 293) established within the NSC a Committee on Transnational Threats to develop strategies to deal with such threats and to assist in the resolution of operational and policy differences among Federal departments and agencies in responding to the threats, to ensure the effective sharing of information about transnational threats among Federal departments and agencies, "including law enforcement agencies and the elements of the intelligence community," and "to develop guidelines to enhance and improve the coordination of activities of Federal law enforcement agencies and elements of the intelligence community outside the United States with respect to transnational threats."

The Attorney General has not been made a statutory member of the NSC, reflecting an intention to keep law enforcement separate from policymaking, defense, and intelligence agencies, although Justice Department representatives are routinely involved in NSC decision making. In a memorandum of February 13, 2001 on the organization of the NSC system, President Bush directed that the Attorney General would be invited to participate in meetings pertaining to his responsibilities, but a formal inclusion of the Attorney General in the NSC was not proposed. The memorandum did indicate that the Justice Department would be represented in the NSC Deputies Committee and Policy Coordination Committees giving DOJ the functional equivalence of membership. The only official with authority over both intelligence and law enforcement efforts is the President, even though in some administrations the National Security Adviser or the White House Chief of Staff may have significant, if nonstatutory, responsibilities. Presidents will have limited time to devote to sorting out jurisdictional responsibilities of various agencies in specific cases, and some observers question the effectiveness of existing mechanisms for balancing international legal and policy concerns. Philip Heymann, a former Deputy Attorney General, has argued that, "Uncertainty is upsetting to both sides. It would be wise for the federal government to propose a statute in an effort to use the weight of legislation to settle open questions .... [T]he Supreme Court is likely to give great deference to the views of the executive and legislative branches on an issue that has such significant national security dimensions."

Distinctions between law enforcement and intelligence can lead to potentially important difficulties. For instance, in March 1997, according to media reports, the FBI, out of concern for an ongoing criminal investigation, was unwilling to share information with the NSC staff about alleged contacts between Chinese officials and U.S. political fundraisers. Reports further indicate that such information was not shared with the Secretary of State, who was then preparing for an official visit to China. Samuel Berger, President Clinton's National Security Adviser was recalled as "sputtering in a profane rage," and his deputy, James Steingberg, subsequently recalled that the problem of insufficient

information-sharing was “commonplace.” Although the absence of this information may not have complicated U.S. diplomacy in this instance, some observers suggest that information regarding other countries’ efforts to influence U.S. policies must be available to those responsible for the formulation and execution of U.S. national security policy. Given the stakes of U.S. relations with China, they suggest that keeping the Secretary of State and other officials responsible for foreign policy uninformed of important initiatives of the government in Beijing may jeopardize important U.S. interests in international negotiations. The FBI is not charged with responsibility for national security policy, and critics argue that a determination by the Justice Department to monopolize information legitimately needed by the NSC or the Secretary of State undermines the constitutional responsibilities of the entire executive branch. In another case, both the Attorney General and the FBI Director were publicly critical of the cooperation received from the government of Saudi Arabia concerning the 1996 bombing of the Khobar Towers housing complex in which 19 U.S. military personnel were killed. Former DCI John Deutch remarked on

> the faintly ridiculous spectacle of Freeh, an individual with impeccable law enforcement credentials, who has successfully battled crime in the United States, being stiffed repeatedly by the Saudis when he requested coequal status in their internal investigation, and expected treatment of suspects and evidence according to American standards. Fat chance—the Saudi royal family’s conception of justice is quite different from our own. In any case, if the situation were reversed, it is highly unlikely that we would let foreign law enforcement officials play a significant role in a sensitive internal investigation of an incident that occurred on

U.S. soil. An area of growing concern is the possibility of attacks on U.S. information systems. Although such attacks thus far have apparently been few in number and without permanent effects, many observers are greatly concerned that significant damage could be inflicted on the computer systems and databases that are depended upon not only by government agencies, but also by important sectors of the U.S. economy. It is difficult to determine the sources of such attacks, whether they originate inside or outside of U.S. territory, or whether they are isolated or part of a larger plan. Resolving such question may be significantly complicated by statutes that assign separate responsibilities to law enforcement and intelligence organizations. An attack launched by a teen-aged hacker from a computer in the United States is clearly a law enforcement matter. An attack by a foreign government on U.S. defense databases would undoubtedly be viewed as a concern for intelligence agencies. In actuality, however, determining the source and purpose of the attack within a reasonable time might be difficult without the involvement of both law

enforcement and intelligence agencies. It is argued that current statutory restrictions can, however, preclude an investigatory role by intelligence agencies if U.S. persons or locales are involved in launching such attacks.

The need for coordinating law enforcement and policy issues is reflected in Presidential Decision Directives (PDDs) (Protection Against Unconventional Threats) and (Critical Infrastructure Protection) of May 22, 1998. The Directives are classified, although summaries have been officially released.62 They established within the NSC staff a National Coordinator for Security, Infrastructure Protection, and Counterterrorism, whose responsibilities include coordination among agencies for policies dealing with terrorism and other threats to U.S. infrastructure. A major focus of these directives is the need to develop plans in conjunction with the private sector that controls a major percentage of U.S. infrastructure, but which may, for a variety of reasons, be reluctant to share plans for infrastructure protection with government officials. The Bush Administration subsequently placed these responsibilities in the NSC Policy Coordination Committee on Counter-Terrorism and National Preparedness. PDD also established a National Infrastructure Protection Center (NIPC) within the FBI to serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. Staffed by law enforcement agency investigators, as well as representatives detailed from other agencies, including the Intelligence Community, the NIPC will be able to provide direct support to DOD or the Intelligence Community, depending upon the nature and level of a foreign threat/attack, protocols established between special function agencies (DOJ/DOD/CIA), and the ultimate decision of the President." NIPC's former Director, Michael Vatis, described the role of this Centre in 1999:

> Thus, the NIPC is housed in the FBI to enable it to utilize the appropriate authorities to gather and retain the necessary information and to act on it. Now, this does not mean that the ultimate response to a cyber attack is limited to criminal investigation and prosecution. The response will be determined by the facts that are uncovered. Thus, for instance, if it is determined that a cyber intrusion is part of a strategic military attack, the President may determine that a military response is called for. But no such determination can be made without adequate factual foundation, and the NIPC's role is to coordinate the process for gathering the facts, analyzing them and making determinations about what is going on, and determining what responses are appropriate.

Sensitive to statutory complexities, the PDD stated that, "All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, *to the extent*

permitted by law." (Emphasis added.) Although a related White Paper indicated that the Administration "shall consult with, and seek input from, the Congress on approaches and programs," there is no indication that the Clinton Administration believed that the existing statutory regime is inadequate for dealing with cyber threats or that a need exists for legislative initiatives. Subsequently, however, there were indications that Clinton Administration officials believed that the government needed greater authorities to trace persons who abuse the Internet. These concerns were addressed in the USA-Patriot Act passed in October 2001 in the wake of terrorist attacks.

In these two directives (the complete texts of which have not been made public), the Clinton Administration established a policy and an administrative structure to deal with critical infrastructure protection and with terrorism. The structure has been maintained by the Bush Administration. It is well understood that ways must be found to encourage cooperation from the private sector, and that there are many difficulties to be overcome in this regard. Some observers argue, in addition, that, in crises involving computer-based attacks on U.S. infrastructure, the separate responsibilities and authorities of law enforcement and intelligence agencies might be impediments to immediate detection or to a rapid response. Other observers suggest that organizational authorities established by classified executive branch directives fail to provide necessary public accountability, and may increase suspicion of government among parts of the electorate traditionally suspicious of government secrecy. Administration spokesmen argue, however, that, given the changing variety of potential threats now facing the country, a flexible structure centred on the NSC staff can enable the Federal Government to choose the best approach in specific circumstances and adapt organizational relationships to changing needs

Self Assessment Exercise

1. Discuss the distinctions between law enforcement and intelligence gathering in relation to potential difficulties.

2. Succinctly discuss some of the technical and administrative recommendations of Elizabeth Rindskopf, towards information flow and data retrieval.

4.0 Conclusion

Post-Cold War realities—geopolitical and technological—challenge not only the statutory foundations of law enforcement and intelligence agencies, but also, more fundamentally, constitutional separations of power. The sorting out of roles and missions, as well as oversight responsibilities, has been under review by the executive branch in recent years, and various coordinative mechanisms have been created. Nevertheless, areas of overlap and uncertainty will undoubtedly remain for some time to come. The law enforcement and national security is especially significant, and penetrates all spheres in any government. Every nation should emphasise security paradigm that fosters

genuine aggressive, active intelligence gathering. It anticipates the threat before it arises and plans preventive action against suspected targets. Similarly, the law enforcement paradigm fosters reactions to information provided voluntarily, uses ex post facto arrests and trials governed by rules of evidence, and protects the rights of citizens.

5.0 Summary

This unit throws light on the division of responsibilities between intelligence and law enforcement agencies reflects this reality based on statutes and executive orders. The behavioural effect of investigations was discussed with cases marked by cultures in the process of gathering security information and formation of interactive relationships. Summarily vast bulk of intelligence collection is, and will likely remain, focused on topics far removed from the concerns of law enforcement agencies, the use of intelligence information has been seen as having important potential advantages with the increasing global scope of much criminal activity.

6.0 Tutor Marked Assignment

What are the contributions of the FBI in securing the United States?

7.0 References/ Further Reading

CRS Report 96-499, *Antiterrorism and Effective Death Penalty Act of 1996: A Summary,* by Charles Doyle , June 3, 1996, pp. 25-30.

Doyle McManus, "FBI Director Objects to Briefing Request," *Los Angeles Times*, March 25, 1997, p. 11.

Jim McGee and Brian Duffy, *Main Justice: The Men and Women Who Enforce the*

John F. Harris and David A. Vise, "With Freeh, Mistrust Was Mutual," *Washington Post*, January 10, 2001, p. A1; see also James Steinberg,

Jonathan M. Fredman, "Intelligence Agencies, Law Enforcement, and the Prosecution

Loch K. Johnson, *America's Secret Power: the CIA in a Democratic Society* (New York: Oxford University Press, 1989), pp. 133-203.

Louis René Beres, "On International Law and Nuclear Terrorism," *Georgia Journal of International and Comparative Law*, Spring 1994, pp. 3-8.

Nation's Criminal Laws and Guard Its Liberties (New York: Simon & Schuster, 1996), pp. 373, 374.

Philip B. Heymann, "Law Enforcement and Intelligence in the Last Years of the Twentieth Century," *National Security Law Review*, Winter 1996, p. 12.

Stewart A. Baker, "Should Spies Be Cops?,"*Foreign Policy*, Winter 1994-1995, pp. 36-37.
Team," *Yale Law and Policy Review*, 1998, Vol. 16, No. 2, pp. 336-337.

UNIT 8
Police Accountability: Evidence from United Kingdom

1.0 INTRODUCTION

In order to understand the complex nature of police accountability in the United Kingdom, it is necessary to map out the terrain of policing across three separate jurisdictions and to highlight a number of themes. From the outset, it is necessary to be clear about what we are referring to when talking about the police of the United Kingdom. The UK police are not a unitary body similar to the national police forces that exist in many parts of the world. In England and Wales, 43 forces undertake territorial policing on a geographical basis. In Scotland there are eight regional police forces. In Northern Ireland, The Police Service of Northern Ireland (PSNI) came into being in November 2001 following the recommendations of the Patten Commission on policing in the province. It replaced the Royal Ulster Constabulary, which itself had been in operation since the disbandment of the Royal Irish Constabulary in 1922.

In addition to the these forces, there are a number of non-Home Office police forces that have a specialised remit and exercise their jurisdiction throughout the UK. These include the British Transport police (BTP); the Ministry of Defence Police (MOD); and the United Kingdom Atomic Energy Authority Constabulary (UKAEA). The Jersey, Guernsey and Isle of Man Police are separate organisations that carry out policing in those islands. Recognising the need to adapt to transnational and cross-border issues, the government and the police service have also developed national policing agencies. In 1998, the

amalgamation of six regional crime squads established the National Crime Squad (NCS). The overall remit of NCS is to target criminal organisations committing serious and organised crime. Also operating nationally is the National Criminal Intelligence Service (NCIS), which was established in 1992 drawing on staff from the Home Office, HM Customs and Excise, the police service and local authorities. In November 2004, the government introduced the Serious Organised Crime and Police Bill. This is intended to bring together the work of NCS, NCIS and other agencies through the creation in 2006 of the Serious Organised Crime Agency (SOCA). Therefore, although on some occasions we might refer to .the police service as if it were a single entity, it continues to consist of a number of police forces. Accordingly the arrangements for police accountability are necessarily complex. In the United Kingdom, accountability has been a consistent and, at times, fiercely debated policing issue. In Northern Ireland the legitimacy of the police has been questioned in a divided society. In England and Wales police accountability during the 1980s became a national political issue concerning who controlled the police, who *should* control them and whether they were beyond democratic control. These issues have lost some of their controversy in recent years as discussion surrounding accountability has shifted to focus on police performance and effectiveness. As commentators have noted, accountability remains significant. This is for the following reasons, the first two of which are especially pertinent in the human rights context:

1. ***The paradox of police governance***: There is a need to balance the unwarranted exercise of coercive power by the police with enabling their effective operation.
2. ***Policing is political***: Policing is about the exercise of power and there are competing options for policing priorities and style.
3. ***Financial stewardship***: The police need to be held accountable for their use of public resources. (The total expenditure on the police in the UK exceeded £12 billion in 2004/5).
4. ***Police legitimacy***: Police in democratic states strive for legitimacy to achieve the active cooperation and trust of the policed. Accountability contributes to the legitimacy of the police. In the chapters that follow, although the policing of the UK comprises three separate systems based on geographic and legal divisions, the primary focus will be on England and Wales, which contains 90% of the UK.s population. Where significant differences exist in the policing systems operating in Scotland and Northern Ireland, these are highlighted.

2.0 Objectives

At the end of this unit, students should be able to:

a. Understand the complex nature of police accountability.
b. Examine International Standards and practices on Policing a nation.

3.0 Main Body

3.1 International Standards on Policing and Accountability

A number of international instruments have considerable relevance to police accountability in the UK. The UN Universal Declaration on Human Rights 1948 is a fundamental source for legislative and judicial practice. As such, it provides human rights principles and standards that underpin the accountability of the police. In 1951, the UK ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms, which endorsed the principles of the UN declaration. The articles of the Convention reaffirm the fundamental freedoms in democratic systems of government. UK law gave effect to the Convention in the Human Rights Act 1998. As public authorities under the Act, the police have a responsibility to abide by the Convention. The Human Rights Act 1998 provides for adjudication by UK domestic courts and for the award of compensation in cases where public authorities have breached Convention rights. Complainants can take cases that the UK domestic courts cannot resolve to the European Court of Human Rights in Strasbourg. These arrangements provide a powerful legal framework making the police accountable for their actions. The Independent Police Complains Commission, and in Northern Ireland the Police Ombudsman, take account of the Human Rights Act 1998, in investigating complaints about police misconduct. Two other measures provide guidance for police as to their conduct. The UN Code of Conduct for Law Enforcement Officials (1979) sets out basic standards for policing agencies across the world and relates to all law enforcement officers who exercise powers of arrest and detention. It requires them to recognise the rights set out in the UN Universal Declaration and other international conventions. In particular, police should only use force when it is necessary. The amount of force should be proportionate to the circumstances. The Council of Europe Declaration on the Police (1979) defined the rules of conduct expected of police in the member states of the Council of Europe, which includes the UK. The rules were designed both to help protect human rights and to improve the status of police officers. In 2001, The Council of Europe supplemented the Declaration by the Code of Police Ethics. The UN Code of Conduct, the European Declaration on the Police and Code of Police Ethics provide basic standards for the operation of legitimate law enforcement. However, they are not directly judicable in law. They should, however, be regarded as guidance which indirectly informs the practice of policing and accountability in the UK.

Statutes and Structures for Police Accountability in the United Kingdom (*the way things are supposed to be)*

The police are subject to the rule of law and to legislation, which is the product of Parliament.

Although judicial processes and case law may affect the interpretation of legislation, and guidelines on procedure may be issued by the executive, the legislature is the origin from which the powers of police are derived. In this sense, they are subordinated to the law and to the law alone. In relation to policy, however, the major public powers of government are vested in ministers who are servants of the Crown. Police also have allegiance to the

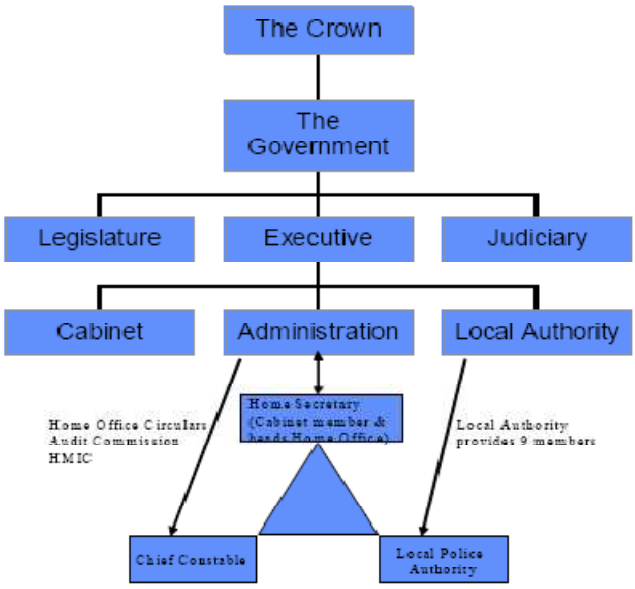
Crown, which serves instead of the state as a central organising principle of government. The arrangements for accountability of the police, therefore, are not simply those of subordination to government. A more complex system of accountability is in operation.

The tripartite system of police accountability

The current system of holding the 43 forces of England and Wales accountable has been characterised as .the tripartite structure of police accountability. Established under the 1964

Police Act, following the deliberations of the 1962 Royal Commission on the Police, this remains the fundamental basis of police governance. The tripartite system distributes responsibilities between the Home Office, the local police authority, and the chief constable of the force. Legislation since the 1964 Police Act, including the 1994 Police and Magistrates. Courts Act (PMCA), the Police Act 1996, and the Police Reform Act 2002, has endorsed the tripartite arrangements, though not always uncontroversial. This tripartite system provides accountability to Parliament through the Home Secretary (who has responsibility for policing policy including centrally set .key priorities. that are formalised within a National Policing Plan). It also provides accountability to local populations through the local police authorities, which comprise of elected local councillors, magistrates and business representatives nominated by a central panel. In practice chief constables also respond to policies and circulars set by the executive (the Home Office and Her Majesty's Chief Inspector of Constabulary). The autonomy of chief constables is arguably limited by the current arrangements, although case-law has made it clear that the police are the servants of the law in terms of their operational discretion, and are not subject to administrative or political direction in this respect. Figure 1 below provides an overview of the tripartite system and where it is situated constitutionally.

Figure 1



One intention of the 1994 PMCA was to strengthen the role of local police authorities by giving them additional powers, including involvement in developing local policing plans. However, the 2002 Police Reform Act moved greater power towards the centre through, *inter alia*, the introduction of the Home Secretary's rolling three year National Policing Plan. Table 1 shows the current balance of powers and the respective responsibilities of the tripartite structure. Scotland, unlike England and Wales prior to the 1964 Police Act, already had a tripartite system of police governance, in which the local authority itself was the local police authority. Nevertheless reforms in England and Wales have followed a similar pattern in Scotland, the primary legislation being the Police (Scotland) Act 1967. Scottish Ministers retain overall responsibility for policing policy. Police Authorities and Joint Police Boards are responsible for setting police budgets and ensuring that best value is attained for the public purse. Chief Constables are responsible for the operational aspects of policing within their force areas. In Northern Ireland, the role of the police authority is taken by the Policing Board, which not only has a responsibility for delivering an efficient police force but is also responsible for helping the Police Service of Northern Ireland (PSNI) fulfil its statutory obligation to meet the standards of the Human Rights Act 1998. The Board also has the power to launch its own inquiry into any aspect of the PSNI.s work, with or without the agreement of the chief constable. This gives it a more active role in the management of the police than is the case with local police authorities.

Table 1:
The tripartite system under the Police and Magistrates. Courts Act 1994 and the
Police Reform Act 2002

Home Secretary/Home Office	Local Police Authority	Chief Constable
Determines key national policing objectives. Produces annual National Policing Plan and presents it to Parliament Directs police authorities to establish performance targets. Can require a police force to take remedial action if HMIC judges them inefficient or ineffective Determines cash grant to police authorities Approves appointment of chief constables Issues statutory codes of practice and directions to police authorities Issues statutory codes of practice to Chief Officers Has authority to order amalgamations	Responsible for maintaining an effective and efficient force Determines local policing priorities. Produces a three-year strategy consistent with National Policing Plan Determines arrangements for public consultation Established as precepting body responsible for budgeting and resource allocation Responsible for appointment and dismissal of the chief constable (subject to ratification by the Secretary of State). Can require suspension or early dismissal on public interest grounds Membership of 17 (usually). 9 from local government 5 local 'independents' 3 magistrates	Responsible for direction and control of the force Responsible for operational control Drafts local policing plan in conjunction with local police authority Responsible for achieving local and national policing objectives Responsible for resource allocation Chief constables and deputy/ assistant chief constables on fixed term contracts

Source: Mawby and Wright 2003.

The Police and Criminal Evidence Act 1984 (PACE)

In addition to the tripartite structure of police accountability and its associated legislation, the police are subject to the Police and Criminal Evidence Act 1984 (PACE). The criminal justice system ensures that suspects apprehended by the police have the right to trial by a jury in serious cases and are given an opportunity to have legal representation. The court system also ensures that the police have followed the correct procedures, for example, those established by PACE 1984. Failure to follow these rules can and does result in failures to secure convictions because the courts increasingly use exclusionary rules to render inadmissible any evidence which has not been fairly obtained. The application of the principle of the fruits of the poisoned tree means that entire cases can fail when the rules have not been followed, with important repercussions for police effectiveness. The statutory powers of police on matters of stop and search; entry, search and seizure; arrest, detention and the questioning of suspects are provided by PACE 1984. Codes of Practice created under the Act govern cautioning procedures, identification parades and a range of other responsibilities. Strictly speaking, the codes are not statutory but any

breach of their requirements amounts to a disciplinary offence. Also, any breach of the codes is admissible in evidence in criminal or civil proceedings against the police. Overlaying the tripartite structure of accountability and the existing legislation on policing is an oversight regime that includes:

Her Majesty's Inspectorate of Constabulary (HMIC)

The first Inspectors of Constabulary were appointed under the provisions of the 1856 County and Borough Police Act (and in Scotland under the Police (Scotland) Act 1857). The Inspectors have independent status, being servants of the Crown and not Home Office employees. Section 38 of the 1964 Police Act (and section 33 of the Police (Scotland) Act 1967) specified the inspector's role and gave them the power to inspect and report to the Home Secretary on the efficiency and effectiveness of police forces. The role of HMIC has since been laid out in the Police Acts (1994 and 1996) and, relating to Best Value, the Local Government Act 1999. The inspectorate's role, according to its *statement of purpose*, is: To promote the efficiency and effectiveness of policing in England, Wales and Northern Ireland through inspection of police organisations and functions to ensure:

- Agreed standards are achieved and maintained;
- Good practice is spread; and
- Performance is improved.

Also to provide advice and support to the tripartite partners (Home Secretary, police authorities and forces) and play an important role in the development of future leaders.8 There are currently six Inspectors (four are former chief constables, two are from non-police backgrounds) with regional responsibilities and three Assistant Inspectors (two seconded deputy chief constables and one from a non-police background (who specialises in race and diversity issues) who provide policy and inspection support. The inspectors conduct their work assisted by staff officers and support staff. The Chief Inspector of Constabulary (HMCIC) coordinates their work and advises the Home Secretary on policing matters. Seconded police officers and Home Office civil servants provide support to the Chief Inspector. In terms of the inspections themselves, HMIC conducts inspections of forces and of the geographic Basic Command Units (BCUs) within force areas. It also conducts thematic inspections that focus on a specific area of policing, such as corruption (*Police Integrity*), visibility and reassurance (*Open All Hours*) and diversity (*Diversity Matters*). With the Audit Commission; it also conducts Best Value inspections.

The Audit Commission (England and Wales)

Since 1988 the police have been scrutinised by the Audit Commission. This independent body was established in 1982 by the Local Government Finance Act to monitor and promote economy, efficiency and effectiveness in the management of local government. The Audit Commission first focussed on the police in 1988 and early reports scrutinised the financing of police funding and budget allocation. However, later reports focused on operational matters, including crime management and patrol work. Although the Commission's

recommendations are not prescriptive, they are commonly implemented, which is no small task. As one retired chief constable has noted, between 1997 and 1999 there were .no less than 27 Audit Commission and Police Inspectorate thematic reports published, incorporating over 300 different recommendations. In Scotland, The Accounts Commission and Audit Scotland are linked independent statutory bodies that ensure the Scottish Executive and public sector bodies are held to account for the proper, effective and efficient use of public money. Audit Scotland publishes an annual report *Police and Fire Performance Indicators* that compares the performance of Scottish Councils.

Best Value

From April 2000, the Best Value programme placed a statutory duty on local authorities to deliver services to clear standards by the most effective, economic and efficient means. Local police authorities are included as .best value authorities and as such police forces are required to demonstrate .best value. Accordingly, police forces must report against a series of Best Value Performance Indicators.

The Police Standards Unit

The Police Standards Unit began work within the Home Office in July 2001, but was formally established by the Police Reform Act 2002. It has become increasingly influential. Its role is to identify good policing practice and the means of spreading it. It also has an intervention role. If a force is identified as requiring .remedial actions, it will intervene to improve performance. In this role, the PSU works closely with HMIC.

The Police Performance Assessment Framework (PPAF)

The PPAF was introduced in April 2004. It has been developed by the Home Office, in consultation with the Association of Chief Police Officers (ACPO) and Association of Police Authorities (APA). It introduced PPAF performance measures and aims to .provide an effective, fair framework for comparing police performance and provide a firm basis for effective performance management. It is therefore intended to be both a means of holding individual police forces accountable for their performance and a means of comparing forces. Performance against each other. According to the Home Office, in addition to focussing on operational effectiveness, the Policing Performance Assessment Framework provides measures of satisfaction plus overall trust and confidence in the police, as well as measures that put performance into context in terms of efficiency and organisational capability. In line with the Government's desire to enhance policing accountability at a local level, performance against national and local priorities, are reflected in the framework. HMIC published its first .baseline assessments. of each force in England and Wales in Summer 2004, which led to much debate (media, public and political) concerning the comparative performance of forces and press speculation over whether chief constables of forces rated as poor would be

dismissed. Parties on both sides of the political spectrum see this kind of public information as a key mechanism for encouraging public scrutiny of the police.

3.2 Financial and Organisational Accountability

In the 1980s, the government applied its public sector Financial Management Initiative (FMI) to the police service. This was concerned with business management strategies and audit techniques and related to financial accountability in the stewardship of public money. The National Audit Office has produced reports on value for money in policing and District Auditors are empowered to undertake audits of the finances of public sector organisations, including the police. The enactment of the Police and Magistrates Courts Act 1994 changed the system of police funding in a way that theoretically provided greater control to the local police authority and greater devolution of budgeting within police forces. Since the 1994 Act each local police authority receives a cash-limited grant from the Home Office, which is supplemented by funding from the local authority raised through the revenue support grant, non-domestic rates and council tax. Forces are also permitted to seek out a relatively small proportion of funding through sponsorship arrangements. The Local Police Authority and the chief constable, rather than the Home Secretary, then decide on the allocation of funds between police officers and civilian staff, equipment, buildings and vehicles. Thus whilst the Home Secretary retains control of the total amount of the grant, police authorities and chiefs have greater freedom within the budget. Devolution of budgeting is therefore being encouraged but not with any over-arching national strategy. It is occurring at a speed and implementation that suits individual forces. These arrangements, through codes of practice, encourage a greater amount of local managerial freedom and delegation of financial responsibilities within the police organisation. Potentially this can support the objective of meeting local priorities, thereby increasing local accountability.

At an organisational level, accountability is provided through a hierarchical rank structure a quasi-military structure aimed to produce a disciplined and answerable service. In addition police officers are subject to a disciplinary code that punishes offences including discreditable conduct, failure to obey orders, racially discriminatory behaviour and falsehood. Offences are investigated internally and judged at disciplinary hearings. Punishments range from reprimand to fine to dismissal. A breach of the code may also constitute a criminal or civil offence. Officers taken through the courts can still face disciplinary boards.

Self Assessment Exercise;

1. Generally police accountability is said to be necessarily complex. Explain
2. Explain the tripartite system of police accountability as obtainable in England.

4.0 Conclusion

As expected and should be practiced, Policing in the UK has been subject to extensive pressure since the enactment of the Police Act 1964. Failures in policing have served to keep it in the spotlight over the years. As a result, the government has instituted a number of measures in response to the need for change and more are likely to be necessary. The development of other agencies for investigation and enforcement also means that the public police, who have been in existence since the early 19th century, are not the only agency now responsible for .policing.. Although much attention will continue to be focussed on the public police in the UK, the accountability of these other .policing agencies also needs constantly to be reviewed. The most effective approach that all police agencies can adopt at times when they are under pressure is to remain open to constructive criticism; to welcome scrutiny and to remain highly accessible to ideas from the public. Although this may be a painful process, ultimately it will result in a stronger community-based policing, which will be able to retain the respect and to secure the help of the public.

5.0 Summary

In this unit, our focus has on The Police and Criminal Evidence Act 1984 (PACE) police accountability, International Standards on Policing and Accountability, the tripartite system of police accountability financial and organisation accountability from the British perspective a model Nigeria Police is structured after.

6.0 Tutor Marked Assignment

Explain the need of police accountability in security of a nation

7.0 References/ Further Reading

Jones, T. (2003) .The governance and accountability of policing in Newburn, T. (ed.) *The Handbook of Policing*, pp. 603-627, Cullompton: Willan Publishing.

Leigh, A., Mundy, G. and Tuffin, R. (1999) *Best Value Policing: Making Preparations*, Policing and Reducing Crime Unit Police Research Series Paper 116, London: Home Office.

Loveday, B. and Reid, A. (2003) *Going Local: Who should run Britain.s police?* London: Policy Exchange.

Mawby, R.C. (1999) .Visibility, Transparency and Police Media Relations. in *Policing and Society*, vol. 9, pp. 263-286.

Mawby, R.C. and Wright, A. (2003) .The police organisation. in Newburn, T. (ed.) *The Handbook of Policing*, pp. 169-195, Cullompton: Willan Publishing.

Morgan, R. (1992) .Talking About Policing., in Downes, D. (ed.) *Unravelling Criminal Justice*, London: Macmillan

Newburn, T. and Jones, T. (1996) .Police Accountability. in Saulsbury, W., Mott J., and Newburn, T (eds.) *Themes in Contemporary Policing* London: PSI.

Neyroud, P. (2003) .Policing and ethics. in Newburn, T. (ed.) *The Handbook of Policing*, pp. 578- 602, Cullompton: Willan Publishing.

Neyroud, P. and Beckley, A. (2001) *Policing, Ethics and Human Rights*, Cullompton: Willan
Publishing.

Oliver, I. (1997, 2nd ed.) *Police, Government and Accountability*, London: Macmillan.
Pollard, C. (1999) .Unnecessary Intervention., *Policing Today*, vol.5, no.4, pp. 26-28.

Turpin, C. (1995*) British Government and the Constitution: Texts, Cases and Materials*, London: Butterworths.

Walker, N. (2000) *Policing in a Changing Constitutional Order*, London: Sweet and Maxwell.

Wright, A. (2000) .An introduction to human rights and policing. in *The Police Journal*, 73 (3): 189-209.

UNIT 9
Internal Strategies for building Police-Community Trust

1.0 Introduction

Law enforcement executives are constantly striving to preserve a positive, ethical image of their departments to the public they are sworn to serve and protect. A community's perception of its local police department, however, is influenced by many variables. Every day, tens of thousands of law enforcement personnel throughout the United States perform honorable and conscientious police work, but irreparable damage may be done to the entire profession from even one remote story of police misconduct or corruption. How each community perceives law enforcement depends on each police department. How the department interacts with its citizens, how accessible it is to the community, and how it manages Internal Affairs issues are integral to the profession overall. It is for these reasons that building and maintaining community trust is the hallmark of effective policing.

Law enforcement officers have accepted a position of visible authority within their communities and are held to a tremendously high standard of honesty, integrity, equity, and professionalism. Public trust in law enforcement may be fleeting if police executives do not continually reinforce sound, ethical policies and procedures to agency personnel and to the public. Law enforcement executives, therefore, bear the responsibility for demonstrating proper behavior, informing the community about their department's role in maintaining honor and integrity within the organization, and building and sustaining a trusting working relationship between the public and the police. Establishing Internal Affairs policies and procedures within an agency is not just important, but essential. If misconduct occurs, the agency should already have measures in place to investigate and address such behavior. Internal Affairs investigations, however, should be but one component of a systemic approach to ethical conduct. If law enforcement executives hire the appropriate staff, deliver ethics training, establish an early intervention system, and properly supervise staff, all of which build trust within their communities, the Internal Affairs process may be necessary only in rare instances.

2.0 Objectives

The major objective of this unit is to examine the best way of building trust between the police and the community they serve. Specifically students are expected to know the basic principle of culture of integrity and strategies therein in ensuring effective confidence in law enforcement agencies and agents.

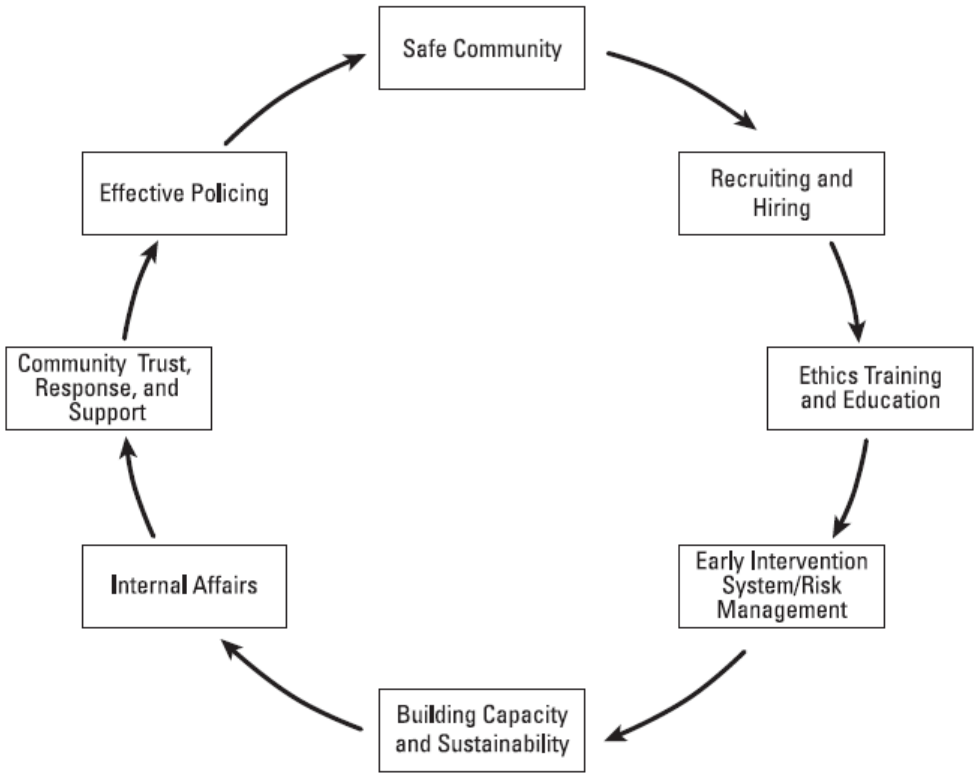
3.0 Main body

Community trust is an established and highly honoured relationship between an agency and the citizens it has been entrusted to serve. It is the key to effective policing, and law enforcement executives bear the primary responsibility for their departments' honesty, integrity, legitimacy, and competence (*Police Integrity,* 1997). To build community trust, it is incumbent on the chiefs of police and managing supervisors to foster an environment within their departments in which ethical behavior is expected and each individual is responsible for meeting those expectations (*Police Accountability and Citizen Review,* 2002). Police chiefs who are transparent (i.e., clear, concise, and open about their department's Internal Affairs process) with their constituencies, acknowledge misconduct, appropriately deal with misconduct when it occurs, and include the public in the response to misconduct will not only obtain, but also sustain, the respect and confidence of the citizens in their jurisdictions. Police departments must adhere to the principles of integrity and professionalism as cornerstones of community trust-building. Because officers occupy a position of trust and confidence in their communities and are afforded awesome authority to carry out their duties, any excessive use of that authority, abuse of power, or failure to fulfil their duties can erode public trust and reduce or destroy their credibility within the communities they serve. Every member of a police department must understand that he or she represents the entire agency, that personal conduct is his or her own responsibility, and that he or she will be held accountable for all conduct, whether positive or negative.

Transparent Internal Affairs processes, although critically important to any agency, are only one building block in maintaining community trust. A department's Internal Affairs practices should always be part of a larger culture of integrity and ethical conduct. If command staff properly supervise officers, the necessity to use the Internal Affairs function should be rare. Culture-changing policies, programs, and training are meaningful and effective not only in preventing misconduct and corruption in the department but also in demonstrating the agency's values and principles. Moreover, the police executive must ensure that the agency's core "values and principles are expressed, communicated, and reinforced throughout all aspects of the department's operations, administration, and service" (*Police Integrity,* 1997, 47). This can be achieved by adopting a clear, precise mission statement that directs the actions of the department. Departmental policies and procedures

must support the agency's mission, and must be written, clearly defined, and enforced. These ethical standards and guiding principles should be set forth in a manual for all personnel and should not only define acceptable standards of conduct, but identify conduct that is unacceptable. These values and principles must be understood and embraced by all executives, supervisors, officers, and civilian employees within the department (*Police Integrity,* 1997).

Figure 1: Internal Affairs in the Context of Community Trust-Building



Creating a culture of integrity within a department is crucial to building and sustaining community trust, effective policing, and safe communities. A clearly defined standard that guides all actions of every member of a department lays the groundwork for a trusting relationship with the community. The chief must model the values and behaviours inherent in a culture of integrity, both internally (through hiring, training, and evaluation) and externally (through community outreach and dialog), as demonstrated in Figure 1.

Internal Strategies for Building Community Trust

Community trust must be built on the foundation of a strong police culture that values integrity and holds individuals accountable for their behaviour and actions. This culture must be modelled by the administration and reinforced by supervisors to be effective. Several components must work together to establish and reinforce that organizational culture. When all elements are in place for a

culture of integrity, a department can be more transparent with its community, and this will help to build a trusting relationship between the two.

Office of Professional Standards

To establish and maintain an ethical, accountable culture within a police department that reflects the core values and guiding principles of the organization, it is critical for the Internal Affairs function to be distinct, yet aligned with, and supported by, the agency's chief executive. In smaller agencies, this may mean that the police chief alone reviews misconduct allegations and complaints. Regardless of staffing resources, the Internal Affairs function should be established in every agency as an Office of Professional Standards (OPS). It can be managed by one person or several, depending on agency personnel resources, but must be distinct because it is an essential unit ensuring behaviour accountability to the agency leadership and the community. Midsize and large agencies may be able to establish and maintain an OPS with dedicated and trained staff who are responsible for building and maintaining a culture of integrity at all levels of the organization through coordination of training and mentoring and through managing Internal Affairs matters. To creatively address personnel allocation and budgetary challenges, smaller agencies should explore the possibility of partnering with other agencies to create a regional OPS that reviews and maintains multiagency ethical standards through an Internal Affairs function. This practice could enhance the professional development of involved staff while sustaining a robust and consistent expectation of professional behaviour and ethical conduct within all participating agencies.

Recruiting and Hiring

It is imperative to recruit and hire individuals who have a service orientation and the character necessary to uphold high standards of integrity, as well as the ability to withstand the temptation to deviate from these standards (*Police Integrity*, 1997). The selection process first must screen out candidates who are not right for the profession, and then it must screen in those who exhibit the most favourable characteristics for the profession and who fit the needs and culture of the local department (*Police Integrity*, 1997). It is important for agency leadership to determine the core competencies that they want their officers to possess, such as compassion and service orientation. Identifying people who will likely excel in a law enforcement career can be accomplished through a combination of medical and psychiatric testing, personal interviews, and background investigations (Delattre, 2006). Researchers have identified five personality characteristics that enable a police officer to perform well: extrovert, emotional stability, agreeable, conscientious, and open to experience. Other variables, such as fitting into an agency's organizational culture and situational factors such as willingness to work in a high-crime area, are equally important when selecting and hiring potential officers (Hughes and Andre, 2007). If a candidate possesses all five personality traits but will not be able to handle the stress of the job, he or she is not a good fit for this type of position.

It is important to have a comprehensive recruiting plan in place, not only to enable an agency to recruit from traditional sources, such as the military, but from other sources such as local colleges and universities. The recruiting plan should also include non-traditional methods of reaching recruits through local news and print media; having officers attend and speak at church activities, school career days, and athletic events; and involving officers in youth programs at the local levels, police athletic leagues, and the Boy/Girl Scouts1 (Delattre, 2006).

One way to recruit competent, ethical, and service-oriented police personnel is through the Discover Policing web site (www.discoverpolicing.org). The Discover Policing web site is the cornerstone of a broad recruitment initiative sponsored by the IACP and the Bureau of Justice Assistance and aimed at enhancing the image of policing. Discover Policing markets the benefits of careers in law enforcement to a broad and diverse audience, from new applicants to those seeking a career change. This resource allows job seekers to look up contact information for nearby agencies and access links to state-specific resources and also provides hiring agencies and prospective applicants with a platform to connect online. Also, hiring agencies can advertise their vacancies at no cost, and candidates are able to post their resumes. Some new hires will come to an agency from another law enforcement department. While it may seem advantageous to hire an officer with field experience, agencies should obtain a thorough reference from the officer's previous employer. An experienced officer seeking to move to a new department may have left his or her previous agency prior to being disciplined or terminated because of misconduct. Unfortunately, departments will often provide a neutral reference for officers with whom they experienced behavioural problems or would have disciplined or terminated had he or she not agreed to resign. This enables problem officers to move from one agency to another without facing the consequences of their inappropriate or poor behaviour. The situation could be avoided if police departments required all new officers to sign an agreement stating that the agency has permission to obtain a copy of the prospective employee's complete employment files from all prior jobs.

Training and Education

The chief of police must establish, model, and support a culture that "promotes openness, ensures internal and external fairness, promotes and rewards ethical behaviour, and establishes a foundation that calls for mandating the highest quality service to the public" (*Police Integrity*, 1997, 48). By doing so, the chief will reinforce desirable behaviour throughout the department, consistent with core values and guiding principles. This effort by the chief is sustained through initial and ongoing training and education at all levels of the organization. Police leaders across the United States have indicated that, in addition to police skills training, it is important to include moral and ethical

decision making throughout an officer's career (*Police Integrity*, 1997). Training in ethics, integrity, and discretion should begin in the police academy and continue on a regular basis until the officer retires. Continued ethics training should include "exercises for the formation and maintenance of good habits and character, as well as exercises in value choices, ethical dilemmas, and discretion in police work" (Delattre, 2006, 52).

Moreover, ethical considerations should be woven into every aspect of training, policies and procedures, and the department's mission. From the most junior recruit to the chief of police, all employees should receive such education and strive to uphold these high ethical standards. The IACP's Code of Ethics can be used in every law enforcement agency to reinforce this standard (*Standards of Conduct*, 1997). Administrative and supervisory training is essential, particularly for new supervisors who are responsible for personnel evaluations. As an adjunct to academy training, the IACP and other police associations provide in-service officer and supervisory training. Local police departments should commit to ongoing training on ethics, supervision, and other related topics from regional police chiefs organizations, state associations of chiefs of police, the National Internal Affairs Investigators Association, and other related organizations. Admittedly, follow-through on such a commitment is based on the agency's training budget, so it is incumbent on police leaders to educate city officials regarding the essential nature of ongoing police training. The COPS Office and other Department of Justice agencies provide free training videos, CDs, and other resources that can augment any training effort. Local colleges and universities are excellent resources for police training because many now offer criminal justice programs. Larger police agencies are often willing to provide seats in their training sessions at little or no cost to help augment a smaller agency's personnel training. All avenues should be considered as chief executives commit to ongoing training for themselves and their officers.

Evaluations and Early Intervention Systems

Consistent, periodic employee reviews and follow-up will address problem behaviour and reduce the need for a law enforcement agency to investigate misconduct or corruption through Internal Affairs. Evaluations enable supervisors to meet with an employee, discuss his or her performance, and formally record strengths, weaknesses, and expectations. Evaluations provide supervisors with an opportunity to encourage and praise desired behaviour and to notify employees when unacceptable behaviour has been reported. Early in the process of recognizing inappropriate attitude or behaviour, the supervisor must communicate his or her concern with the officer, offer assistance, and explain that the agency will expect positive change from the officer (Kelly, 2003). The emphasis is to identify a problematic behaviour or attitude and help the officer correct it as soon as possible. It also is important to let the officer know that positive contributions to the organization and community are valued and that such behaviour can be acknowledged and that negative behaviour can

be addressed. In the case of poor performance, the supervisor can develop a Performance Improvement Plan, identify the specific areas of concern, and use the plan to address and overcome the noted deficiencies (Noble and Alpert, 2009). The plan should be used as positive reinforcement, helping the employee rectify and prevent unacceptable behaviour. Supervisors must conduct follow-up between evaluation meetings to ensure that the officer's performance and accountability continue to improve.

Most often used within the context of Internal Affairs, Early Intervention Systems (EIS) and Risk Management Systems are effective in identifying, addressing, and preventing problem behaviour before it escalates to a matter for Internal Affairs. EIS, which come in many forms, are a series of interrelated personnel management processes that help supervisors identify, assess, and evaluate employees' performance for the purpose of addressing potential concerns in a timely manner. Part of a larger effort to raise the level of accountability in a police department, an EIS is a valuable way to collect and analyze data on an officer's performance, ensuring integrity at all levels of the agency (Hughes and Andre, 2007). An EIS, however, not only reveals unacceptable performance, it should also identify exemplary performance. While an EIS helps an officer in a non-punitive way (e.g., referral to counselling or training), it also should reward outstanding behaviour through awards or promotions. Most EIS use computer systems or databases to track employee records and are housed as a separate entity from the disciplinary system, usually within Internal Affairs units (Walker, Milligan, et al., 2006). The EIS records are intended to track employee behaviours and interventions by supervisors, should that become necessary. As data-driven mechanisms of accountability, these programs rely on a broad array of performance indicators, including use-of-force incidents, citizen complaints, department and community commendations and awards, court appearances, and arrest reports. Supervisors must be adequately prepared to review the data and, as with traditional performance evaluations, conduct appropriate interventions and follow-up with the employee (Walker, 2003). Through an EIS, many behaviour problems could be reduced significantly, resulting in a decrease in the caseload of the Internal Affairs unit.

Self Assessment Exercise

a. What do understand by the concept 'culture of integrity'?
b. How can it be maintained in the quest for law enforcement?

4.0 Conclusion

This unit emphasis the need to bridge the gap between police officers and the community they serve. Similarly the duality of purpose within which law enforcement agents operate as member of the community first and foremost and as members of a separate organisation formed by the society was discussed as well as the various ways of ensuring that credible officers are

recruited into law enforcement organisations; and the mechanism in place to ensure continuous integrity.

5.0 Summary

Building and maintaining community trust is the cornerstone of successful policing and law enforcement. The building and maintenance of trust takes a great deal of continuous effort. Unfortunately, the ethical work of thousands of local law enforcement officers is easily undone by the actions of one unethical officer. Often, the indictment of one seems like an indictment of all. Once misconduct occurs, the Internal Affairs function of the law enforcement agency becomes the primary method of reassuring the community that the police can and will aggressively address and resolve unethical behaviour.

6.0 Tutor Marked Assignment

List and explain five personality characteristics that enable a police officer to perform well.

7.0 References/ Further Reading

Chermak, S. and A. Weiss. *Marketing Community Policing in the News: A Missed Opportunity?* Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, July 2003. www.ncjrs.gov/pdffiles1/nij/200473.pdf

De Angelis, J. and A. Kupchik. *Officer Satisfaction with the Denver Police Complaint Process: A Comparison of the Baseline and Post-Implementation Surveys*. Conducted for the Office of the Independent Monitor, Denver, Colorado: 2007. www.denvergov.org/Portals/374/documents/OfficerSatisfaction2006.pdf

Fields, C. *1999–2006 Award-Winning Community Policing Strategies; A Report for the International Association of Chiefs of Police, Community Policing Committee*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2007. www.cops.usdoj.gov/files/RIC/Publications/e08071596.pdf

Walker, S., S.O. Milligan, and A. Berke. *Strategies for Intervening with Officers through Early Intervention Systems: A Guide for Front-line Supervisors*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, Police Executive Research Forum, February 2006. www.cops.usdoj.gov/files/RIC/Publications/e01060004.pdf

www.discoverpolicing.org:.*A Leadership Guide for State, Local, and Tribal Law Enforcement*

Reiter, L. *Law Enforcement Administrative Investigations: A Supervisory and Agency Guide*
to: Handle Citizen Complaints of Misconduct, Conduct Administrative Investigations, Manage the Internal Affairs Function, and Create Reasonable and Defensible Discipline 2nd Edition. Tallahassee, Florida: Lou Reiter and Associates, 2004.

Thurnauer, B. *Best Practice Guide, Internal Affairs: A Strategy for Smaller Departments*.
Alexandria, Virginia: International Association of Chiefs of Police, 2002.
www.theiacp.org/LinkClick.aspx?fileticket=4B%2f4SDZtgV8%3d&tabid=392

U.S. Department of Justice, Office of Community Oriented Policing Services and Office of
Justice Programs, National Institute of Justice. *Police Integrity – Public Service with Honor,*
A Partnership Between the National Institute of Justice and the Office of Community riented
Policing Services. Washington, D.C., January 1997.
www.ncjrs.gov/pdffiles/163811.pdf

Fisher-Stewart, G. *Community Policing Explained: A Guide for Local Government*.
Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing
Services and International City/County Management Association, 2007.
www.cops.usdoj.gov/files/RIC/Publications/cp_explained.pdf

Hackman, M. J. *Citizen Complaints About Police Use of Force: Bureau Justice of Statistics*
Special Report. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs,
2006. www.ojp.gov/bjs/pub/pdf/ccpuf.pdf

"Investigation of Employee Misconduct: Concepts and Issues Paper." International
Association of Chiefs of Police, National Law Enforcement Policy Center, Alexandria,
Virginia: 2007.

UNIT 10
External Strategies for Building Community Trust

1.0 Introduction

Ongoing community partnerships and dialog help department leaders gauge the communities' perception of the police department and help foster trust between the community and the police. When a chief maintains a continuous dialog with the members of his or her community regarding their perception of how the agency is adhering to established standards, both the police and community leaders gain a better understanding of the community perception and can act to have a positive impact on that perception. Many strategies exist for engaging in effective community outreach with the goal of enhanced community trust, for example, circulating community safety surveys that accurately measure community perception and needs. Such an effort requires a commitment by the police leader to engage the community and respond to its needs.

2.0 Objectives

At the end of this unit, students should be able to understand the concept and philosophy behind community policing and other strategies in place in ensuring effective law enforcement in modern day Security.

3.0 Main body

Community Oriented Policing

A valuable and effective way for a department to engage its community is by practicing community oriented policing. Organizational transformation, problem-solving, and community partnerships comprise the concept known as community oriented policing (Fisher-Stewart, 2007). In existence for more than 30 years, community oriented policing is a policing philosophy that promotes and supports organizational strategies to address the causes, and reduce the fear of, crime and social disorder through problem-solving tactics and community/police partnerships. There is no single set of rules or a specific checklist for what constitutes a community oriented policing program; rather, the philosophy requires citizens and police to collaborate to proactively increase public safety within the community (Fisher-Stewart, 2007). Each

community policing program is as unique as the community in which it is practiced; however, law enforcement agencies have cited five consistent key elements of an effective community oriented policing program (*Protecting Civil Rights*, 2006):

1. Adopting community service as the overarching philosophy of the organization.

2. Making an institutional commitment to community policing that is internalized throughout the command structure.

3. Emphasizing geographically decentralized models of policing that stress services tailored to the needs of individual communities rather than a one-size-fits-all approach for the entire jurisdiction.

4. Empowering citizens to act in partnership with the police on issues of crime and more broadly defined social problems, for example, quality-of-life issues.

5. Using problem-oriented or problem-solving approaches involving police personnel working with community members.

In addition to the five key elements, it is imperative that the chief of police demonstrates his or her commitment to the philosophy and incorporates it into the department's overall mission and way of doing business. Research shows that community oriented policing has greatly improved the public's perception of police. Community oriented policing strategies can establish frequent contact and build more meaningful relationships with the community by fostering dialog between the police and residents and enhancing community trust. Some examples of successful strategies include the following:

- Convene monthly meetings with community members

- Increase bicycle and foot patrols on community streets

- Engage specific sectors of the community, such as schools, minority communities (particularly those who previously have felt disenfranchised), and faith-based Organizations

- Establish programs that solicit involvement from residents, such as Neighbourhood Watch and Night Out Programs.

Citizen Police Academies

Another way for law enforcement to foster community trust is through citizen police academies. Citizen police academies enable residents to learn about their local law enforcement agency's culture and core values and the overall

operations of a department. Citizen police academies provide citizens with a first-hand look at the mission, policies, and regulations to which officers must adhere, and allow them to better understand the job of being a police officer, including the stresses of the occupation (see National Citizens Police Academy Association, www.nationalcpaa.org). Graduates of citizen police academies often become advocates and ambassadors of police policy and practices to fellow citizens. This is an effective way to enhance the relationship between the public and law enforcement.

The Media

Proactively engaging the local media can be an effective way to influence community perception of a police department. Whether a department has a specifically designated public information officer, the agency always has a spokesperson who should use his or her media contacts to conduct a broad, proactive outreach strategy, disseminating information about successful programs within the department. Building rapport with the media will also provide the department with more opportunities to highlight positive stories in the future. By publicizing a community oriented policing or citizen police academy program through the news and print media, a police department can further convey its mission and core values to the public (Chermak and Weiss, 2003).

Implementing Community Trust-Building Activities

Internal Strategies Institute culture-changing policies, programs, and training to solidify the department's core values and ethical principles. Consider developing an Office of Professional Standards to manage these activities. Develop a comprehensive recruiting plan; recruit and hire people with a service orientation. Provide continuous training in ethics, integrity, and discretion to every officer from the time he or she enters the police academy through the time of retirement. Conduct consistent evaluations and review of all employees, and immediately address negative behaviour and reward positive behaviour. Use some form of Early Intervention System, not only in Internal Affairs, but to prevent behaviour that may lead to an Internal Affairs complaint and investigation. External Strategies Institute some form of community oriented policing program to better engage the community. Develop a citizen's police academy. Use the media to publicize positive programs and stories about the department. Hold workshops on subjects of interest to the community. Conduct a community survey to gauge and enhance public perception. Proactively involve the public.

Seminars, Publications, and Surveys

Many law enforcement agencies across the country have used innovative ways to reach out to their communities. Some agencies have held 1-day workshops and seminars on subjects such as community oriented policing and proper use of force. Some agencies have canvassed neighbourhoods, handing out

pamphlets and brochures about the department's programs or local crime statistics. Others have posted billboards with hot line and other important numbers at the police department, while others have posted pertinent information on their web sites or in their annual reports (Chermak and Weiss, 2003). Additionally, many agencies conduct community surveys every few years. A community survey can serve two purposes:

1. it can gather information about the public perception of the agency and

2. it promotes the understanding that the police department is interested in the community, seeks out and listens to community opinions and needs, and is responsive to the community

Citizen Involvement

Often implemented as a result of a local crisis, such as police misconduct, and usually associated exclusively with the Internal Affairs process in the form of a citizen review board, citizen involvement can be used as a tool that fosters continuous dialog between residents and the police department. By formally engaging community leaders in appropriate internal decision-making (e.g., where to implement Neighbourhood Watch programs or whether it is necessary to start a Senior Citizen Alert program), residents will feel that they have a stake in programs that the police may implement, that the police are transparent in their motivations, and that they are assisting the police in improving public safety. If citizen involvement is used only in response to misconduct or corruption, citizens are likely to feel isolated and wary of law enforcement. If they feel included through collaboration, though, they will gain a broader appreciation of police work and gain insight into, and consequently trust of, law enforcement (Delattre, 2006).

Trust is built when citizens feel that the police department listens and appropriately responds to their valid concerns and opinions. Confidential information should not be shared with citizens; however, involving them in even the smallest facet of the organization goes a long way toward instilling a sense of community trust.

Self Assessment Exercise

What are the motives behind community policing

4.0 Conclusion

Community oriented policing is a strategy with a great capacity of improving public's trust perception of police. It brings both the community and the police together as a family, through regular consultations and dialogues, revealing the needs of the community and information flow for better operation on the side of the police in securing the community.

5.0 Summary

This unit brings to the fore how best trust can effectively be built between the police and the community in which they operate through various internal and external means and medium such as community policing, Citizen Police Academies, the media, Seminars, Publications, and Surveys

6.0 Tutor Marked Assignment

What are the strategies involved in effective community policing philosophy?

7.0 References/ Further Reading

Chermak, S. and A. Weiss. *Marketing Community Policing in the News: A Missed Opportunity?* Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, July 2003. www.ncjrs.gov/pdffiles1/nij/200473.pdf

De Angelis, J. and A. Kupchik. *Officer Satisfaction with the Denver Police Complaint Process: A Comparison of the Baseline and Post-Implementation Surveys*. Conducted for the Office of the Independent Monitor, Denver, Colorado: 2007. www.denvergov.org/Portals/374/documents/OfficerSatisfaction2006.pdf

Fields, C. *1999–2006 Award-Winning Community Policing Strategies; A Report for the International Association of Chiefs of Police, Community Policing Committee*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2007. www.cops.usdoj.gov/files/RIC/Publications/e08071596.pdf

Walker, S., S.O. Milligan, and A. Berke. *Strategies for Intervening with Officers through Early Intervention Systems: A Guide for Front-line Supervisors*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, Police Executive Research Forum, February 2006. www.cops.usdoj.gov/files/RIC/Publications/e01060004.pdf

www.discoverpolicing.org:.*A Leadership Guide for State, Local, and Tribal Law Enforcement*

Reiter, L. *Law Enforcement Administrative Investigations: A Supervisory and Agency Guide to: Handle Citizen Complaints of Misconduct, Conduct Administrative Investigations, Manage the Internal Affairs Function, and Create Reasonable and Defensible Discipline 2nd Edition.* Tallahassee, Florida: Lou Reiter and Associates, 2004.

Thurnauer, B. *Best Practice Guide, Internal Affairs: A Strategy for Smaller Departments*.

Alexandria, Virginia: International Association of Chiefs of Police, 2002. www.theiacp.org/LinkClick.aspx?fileticket=4B%2f4SDZtgV8%3d&tabid=392

U.S. Department of Justice, Office of Community Oriented Policing Services and Office of
Justice Programs, National Institute of Justice. *Police Integrity – Public Service with Honor,*
A Partnership Between the National Institute of Justice and the Office of Community riented
Policing Services. Washington, D.C., January 1997.
www.ncjrs.gov/pdffiles/163811.pdf

Fisher-Stewart, G. *Community Policing Explained: A Guide for Local Government.*
Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing
Services and International City/County Management Association, 2007.
www.cops.usdoj.gov/files/RIC/Publications/cp_explained.pdf

Hackman, M. J. *Citizen Complaints About Police Use of Force: Bureau Justice of Statistics*
Special Report. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs,
2006. www.ojp.gov/bjs/pub/pdf/ccpuf.pdf

"Investigation of Employee Misconduct: Concepts and Issues Paper." International
Association of Chiefs of Police, National Law Enforcement Policy Center, Alexandria,
Virginia: 2007.

UNIT 11
Internal Affairs as an Effective Tool for Building Trust

1.0 Introduction

Community outreach and collaboration, as detailed in the previous unit, are valuable tools in developing community trust. Internal Affairs, however, also plays an important role in the relationship between the public and the police. Internal Affairs is a function within a law enforcement agency that investigates allegations of misconduct, corruption, inappropriate adherence to policies and procedures and to behaviour, and matters so assigned by superior officers to ensure the professional integrity of the department and its members. Internal Affairs should be part of the OPS in midsized and larger agencies and should have an integral role in smaller agencies.

2.0 Objectives

This unit is expected to guide students in knowing the basic principles ensuring professional/behavioural integrity in the internal affairs of law enforcement agencies as well as the various procedures of laying down complaints and the investigation processes in general.

3.0 Main body

"The vast majority of law enforcement officers are honest, loyal, and hardworking professionals" (*Investigation of Employee Misconduct*, 2007, 1); nevertheless, a small number of officers become susceptible to misconduct, and when this occurs, community trust in police is eroded. Whether the misconduct is administrative or criminal in nature, the police department must be "able to effectively identify, investigate, discipline, and control their officers to uphold the high standards of integrity central to the policing mission" (Noble and Alpert, 2009, 2). That is when the Internal Affairs process is a necessary tool, not only to address an officer's misconduct, but to regain and maintain the trust of the public.

Effective Internal Affairs processes ensure that complaints about an officer are heard and dealt with effectively within the department, and that an officer is protected against false or malicious accusations through fair, thorough, accurate, and impartial investigations (Noble and Alpert, 2009). A strong Internal Affairs function should both improve morale within an agency and increase trust within the community. The chief of police and all supervisory staff must be steadfast in their commitment to the Internal Affairs process. The procedures for accepting and investigating both internal and external complaints against an officer must be fair, consistent, and timely (*Investigation of Employee Misconduct*, 2001). The department should have written policies and procedures in place about the administration and investigation of Internal Affairs issues and the chief of police must ensure that all Internal Affairs rules and procedures are strictly enforced. A standard for Internal Affairs is in Chapter 52 of *Standards for Law Enforcement Agencies: A Management Improvement Model through Accreditation* (2006), a publication of the Commission on Accreditation for Law Enforcement Agencies (CALEA). The

guidance from that chapter ranges from to whom the Internal Affairs position or division reports to reporting findings at the conclusion of an investigation.

There is no one-size-fits-all approach to Internal Affairs. The key is to ensure accountability in the agency. The methods for achieving this vary by the size of the department, the existing risk management tools in use, the type of misconduct, and the unique characteristics of the community (Noble and Alpert, 2009). Whether a department has a stand-alone Internal Affairs division, a designated supervisory officer, an external oversight agency, or any combination of the three, there are several guiding principles that any department should follow.

The Structure of Internal Affairs

If internal investigations are conducted in house, the physical location of the Internal Affairs function and related documents is of critical importance. It should always be housed in a private, secure area. "The best location for Internal Affairs would be a facility completely separate from the police facility. Complainants, witnesses, and subject officers could appear for interviews and interrogations without their appearances known by the entire department" (Noble and Alpert, 2009, 13). In reality, however, this is feasible only in larger agencies. Many law enforcement executives demonstrate the importance and seriousness of the Internal Affairs function by symbolically placing the unit or person near the executive staff offices (Noble and Alpert, 2009). Similarly, the chief of police (or his or her designee) should directly oversee Internal Affairs matters, further ensuring confidentiality of records and the integrity of the process (*Investigation of Employee Misconduct*, 2007).

Selecting the right person or persons to serve as Internal Affairs staff is crucial. The chief of police must select officers who want to be a part of the Internal Affairs function; an officer should never be forced into this position. The investigator must be well respected in the department, by union officials (if applicable), and in the community; have good interpersonal skills; have significant patrol and supervisory experience; and be fair, objective, and honest. Whoever is selected to serve in Internal Affairs must possess highly advanced investigation skills similar to those used in conducting criminal investigations. Even the most skilled investigator should receive additional and continuous training, not only on the subject of investigations but also in the areas of state employment law, the applicable collective bargaining agreement, and related topics (*Investigation of Employee Misconduct*, 2007). The chief of police must send a clear message about the importance of Internal Affairs by having those personnel report directly to the chief. Moreover, the top executive should reward fair and thorough internal investigators with promotions, commendations, conference attendance, and public recognition of the good work of the officer(s). By sheer necessity, the chief of police in a smaller agency may be responsible for conducting all Internal Affairs investigations and determining the appropriate dispositions. The executive must determine

whether he or she can continue to administer the agency while fairly and thoroughly investigating individual cases. Chiefs should be cautious of creating the perception of impropriety because he or she will be forced to both investigate the allegation and rule on its outcome.

An alternative way for an agency to handle complaint allegations is for the chief of police to ask the subject officer's immediate supervisor to investigate the issue and recommend an outcome to the executive, who will ultimately make the final determination. Usually, the employee's supervisor will conduct investigations into complaints of rudeness, minor neglect of duty, failure to appear in court, failure to follow proper procedure, and other less-serious accusations (Noble and Alpert, 2009). For this method to be effective, however, extensive training for supervisors is required. Last, when a complaint allegation involves the chief executive or a member of his or her executive staff or when there are not enough resources to conduct an internal investigation, an agency can use an external investigator or investigative agency to handle the complaint. The external investigator can be another law enforcement agency, like the state police or the prosecutor's office, or a contract investigator. Some smaller agencies have formed regional Internal Affairs consortiums, while others have established state investigatory associations.

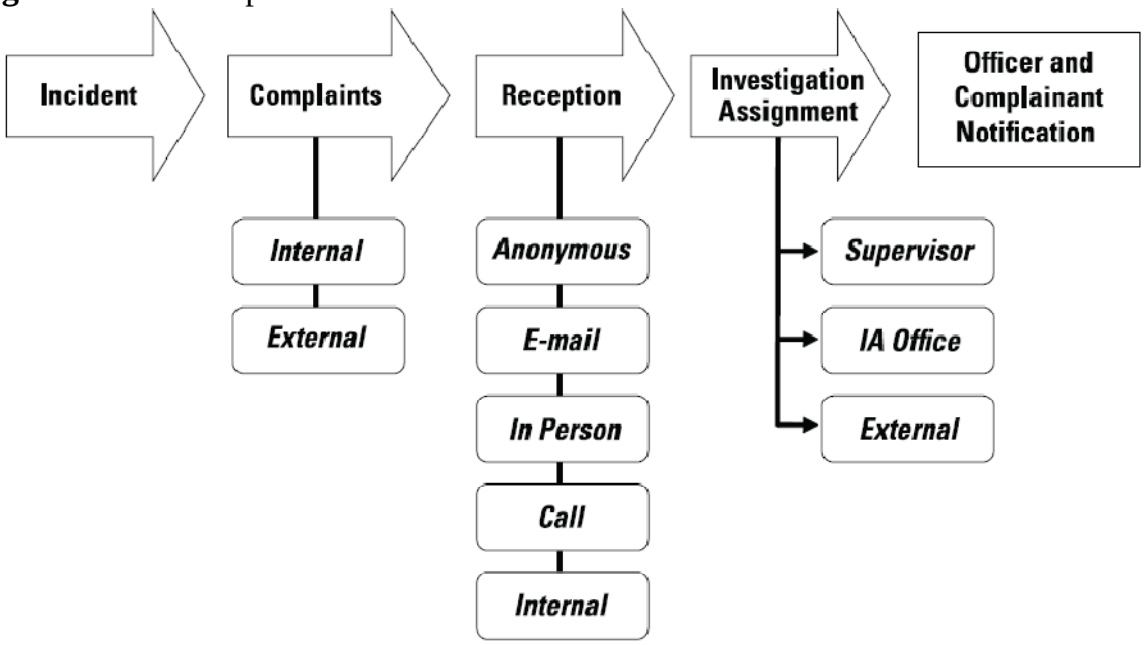
Both models allow law enforcement organizations to conduct another agency's Internal Affairs investigations, providing more support and structure throughout the process. These models also reassure the community of fairness and impartiality. If a department chooses to use an outside investigator or agency to conduct the investigation, that person or agency must be independent, unbiased, and knowledgeable in the areas of law enforcement and employment law. Additionally, the department and the external investigator should enter into a memorandum of understanding (MOU) that sets forth the parameters of the investigation (e.g., timeline, to whom the investigator reports, and the limits on his or her authority with respect to agency staff/ witnesses). The MOU should make it clear that the investigator maintain the utmost confidentiality in the matter and adhere to all applicable laws and collective bargaining agreements. The law enforcement executive should always retain his or her right to release information to the public and should never assign that authority to anyone else. Finally, the external agency should provide frequent progress reports to the chief of police. These reports should not reveal details of the investigation but rather details about the progress of the investigation; for example, which witness the investigator interviewed or when the investigator reviewed a security tape of the alleged incident (Noble and Alpert, 2009). Regardless of which investigatory method is used, a high level of quality control is essential to any fair and thorough investigation. Some basic steps to ensure quality control are set forth in the following section.

The Complaint Process

> "The complaint process should not discourage, dishearten, or intimidate complainants, or give them cause for fear" (*Internal Affairs Guidelines,* 2008, 10)

A complaint is an expression of displeasure with the actions or services of an agency and/ or its employer, or an allegation of wrongdoing. Receipt of a complaint will initiate the Internal Affairs process, so a procedure for complaints must be established. A general model of the complaint process is detailed in Figure 1 and in the text that follows. It is imperative to not only have procedures in place for fairly and impartially accepting, processing, and investigating complaints concerning allegations of employee misconduct but also to inform all police employees and the public of that process (*Investigation of Employee Misconduct,* 2007). "An accessible, fair, and transparent complaint process is the hallmark of police responsiveness to the community" (*Protecting Civil Rights,* 2006, 81). It is incumbent on the police department to make its citizens aware that a complaint process exists, how to file a complaint, and how the agency processes and investigates complaints.

Figure 1: The Complaint Process



Principles of an Effective Complaint Process

An effective complaint process contains the following four underlying principles (*Protecting Civil Rights,* 2006):

1. Comprehensive

A department must investigate all misconduct complaints, regardless of the source (*Investigation of Employee Misconduct,* 2007). CALEA Accreditation Standard No. 52.1.1 states that a written directive must require that "all complaints against the agency or its employees be investigated, including anonymous complaints." A standard practice of accepting any and all complaints is the best way to ensure that any method of complaint is accepted (Thurnauer, 2002). Complaints should be accepted in all forms, including in person, in writing, by e-mail and web pages, or by telephone. Some agencies have even established 24-hour complaint hot lines (Noble and Alpert, 2009).

2. Accessible

Employees and civilians alike should be made aware, through proactive outreach programs, of their right to file a complaint. CALEA Accreditation Standard No. 52.1.4 states that information on registering complaints must be made available through the media and community outreach. Many agencies use brochures (in multiple languages, where applicable), their web sites, and community meetings to let the public know that
the process exists.

3. Fair and Thorough

Departments should afford each complaint "a thorough, rigorous, unbiased, and timely investigation" (*Protecting Civil Rights,* 2006, 89). There should be a standard of fundamental fairness in the investigation of a complaint. All subject officers should be treated equally and be afforded comprehensive
investigations into any claims of misconduct.

4. Transparent

There should be a formal process for all employees to be able to accept complaints at any of the police department's facilities, including substations, satellite offices, and oversight agencies (Noble and Alpert, 2009). All department staff must fully understand the Internal Affairs process and the department should make every effort to inform their constituents about the process. All employees should be trained on what to do when a complainant files a complaint, and the department should have a formal way to keep the complainant apprised of the progress of the complaint (*Protecting Civil Rights,* 2006). Both the IACP and CALEA have adopted standards for written policies and procedures for internal and citizen complaints.4 In addition to the IACP and CALEA standards, many agencies follow similar state certification standards. Whatever standards a department follows, it is important to note that before any type of complaint process is implemented, state and local laws and any collective bargaining agreements that may be in effect must be examined to ensure proper adherence to legal and contract rights.

Once a complaint is received, it should be forwarded to the appropriate personnel (i.e., the Internal Affairs unit, staff member who is in charge of Internal Affairs, or immediate supervisor); recorded, preferably electronically;

and kept in a separate, secure storage area, apart from other personnel records (CALEA, 2006, 52.1.2). As the complaint progresses through the process, it should be tracked, electronically when possible (Noble and Alpert, 2009). Unless a criminal investigation would prohibit it, the subject officer should be notified in writing of the complaint immediately. The notification must contain the rights and responsibilities of the employee with respect to the investigation (CALEA, 2006, 52.2.5). If the state has a codified Officer's Bill of Rights, it should also be included with the notification. Additionally, the notification should include the nature of the allegations; a copy of the complaint, if available; and the name and rank of the officer or the name of the agency that will investigate the claim (Thurnauer, 2002). The entire process should embrace the notion of fundamental fairness. All employees who receive a complaint against them, regardless of rank or tenure, should be treated fairly and equitably.

It is essential to have a written directive that delineates which types of complaints will be investigated by the subject officer's supervisor and which will be referred to Internal Affairs (CALEA, 2006, 52.2.1). Usually, less-serious complaints are handled by the chain of command, while more serious allegations are reviewed by the Internal Affairs function. Even if Internal Affairs is involved, the employee's supervisor should be notified.

Examples of Complaint Categories

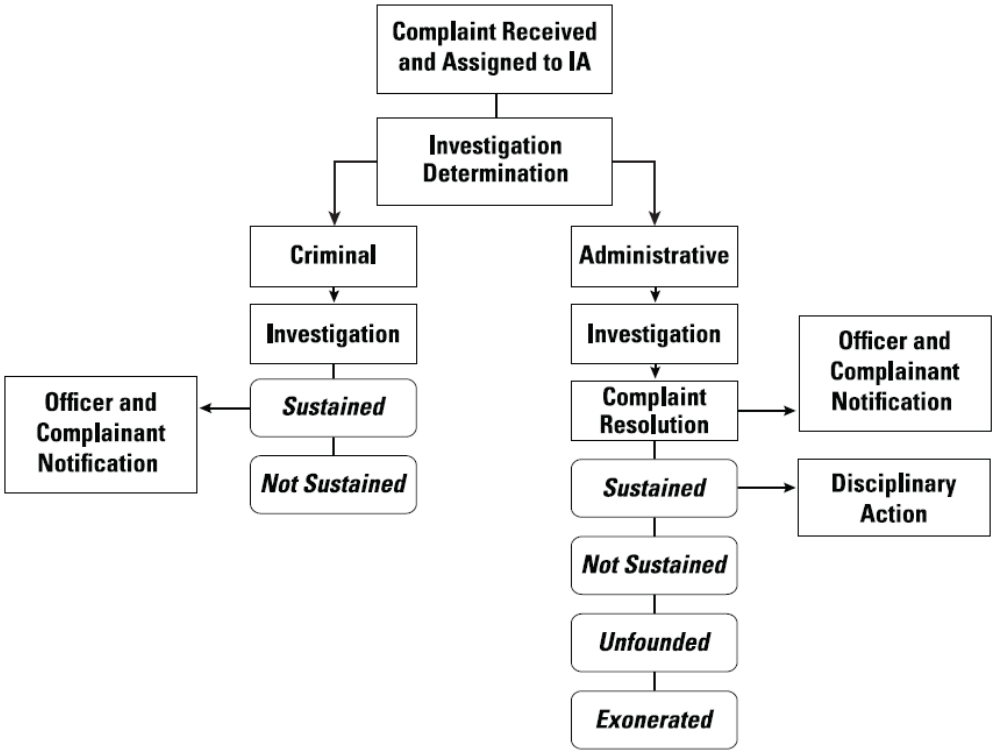
i. Verbal abuse
ii. Physical abuse
iii. On-duty
iv. Off-duty
v. Drug and alcohol
vi. Informal complaints
vii. Traffic citation complaints
viii. Shooting incidents
ix. Violation of policy/procedure
x. Profiling
xi. Violation of policy/procedure.

Once the investigator is assigned, the department sends a letter to the complainant acknowledging receipt of the complaint. The letter should contain the name and contact information of the investigator and explain that the complainant will receive periodic status reports about the investigation and notice of the ultimate disposition within a reasonable time frame (CALEA, 2006, 52.2.4). CALEA Accreditation Standard No. 52.2.3 dictates that a police department must have a written time frame for completing all Internal Affairs investigations. Having a time frame established enhances accountability for a timely response to both the complainant and the officer.

The Investigation

Once a complaint has been received and assigned to an investigator, the investigation process can commence. A general model of the investigation process is detailed in Figure 2 and in the text that follows.

Figure 2: The Investigation Process



At the beginning of the investigation, the investigator must determine if the complaint is valid and, if so, he or she must classify the complaint as either administrative or criminal in nature. If the investigating officer determines that the complaint is frivolous or specifies an action that is made in accordance with agency policy and procedure, the complaint should be dismissed (Noble and Alpert, 2009). If the investigating officer has reason to believe that the allegations are reasonable, he or she should classify the complaint as administrative or criminal and begin the investigation (Noble and Alpert, 2009). If the complaint reveals both administrative and criminal behaviour, the matter should be separated into two investigations, one administrative and one criminal, with a separate investigator assigned to each investigation. Each type of investigation must follow the letter of the law as well as agency policy and procedure, while being careful not to compel statements from the subject officer that may be used against him or her in the criminal investigation (Noble and Alpert, 2009).

After the complaint has been categorized as either criminal or administrative and the subject officer has been notified, the investigator can begin a thorough, unbiased, and timely investigation into the allegation. Information obtained

from all sources, including mobile data terminals, witness interviews, photographs, and canvassing of the scene should be explored. Interviews should not take place in a group setting and should be conducted as close to the incident in question as possible (Noble and Alpert, 2009, 44). Absent restrictions dictated by law or union contract, the department should give the subject officer advance warning before an administration interview, allowing the officer to obtain legal (or union) representation, if he or she wishes (*Internal Affairs Guidelines*, 2008). The investigator must adhere to the investigatory timeline used by the agency. Many agencies have a policy that sets a 30-day time frame of completion from the date the complaint is received. Particularly for smaller agencies, such a timeline may put undue strain on an internal investigator.

All departments, therefore, should have a policy that allows an investigator to request additional time to complete the investigation. If the investigation cannot be completed within 30 days, the chief of police should grant an extension and immediately notify the subject officer and complainant of the extension. The entire investigation process should be transparent to the subject officer and the complainant, and they should be updated regularly on the progress of the investigation. If a collective bargaining agreement is in place, the investigator must adhere strictly to the procedures set forth in the agreement and a designated union representative should also receive periodic updates. It is crucial to note that an investigator should never be a witness in a case that he or she is investigating.

Once the investigation is complete, the investigator should analyze the issues, evidence, testimony, and materials; logically organize the presentation of facts; and write a comprehensive report. The report should include a summary of the complaint, identification of the subject officer, identification of all witnesses, the details of the allegations, the policies and procedures that were allegedly violated, and an extensive narrative about the substance and process of the investigation (Noble and Alpert, 2009). It is advisable to use a uniform report outline in a consistent manner.

The Disposition

The investigator must forward his or her report first to the subject officer's supervisor and then to the chief of police. Usually, the chief is responsible for determining the final disposition in the matter, but he or she can delegate this authority. Findings should consist of at least the following four determinations:

1. Unfounded: the allegation was false or devoid of fact.
2. Exonerated: the act occurred but was lawful and within policy.
3. Not Sustained: the evidence was insufficient to either prove or disprove the allegation.
4. Sustained: the evidence was sufficient to prove the allegation. (*Investigation of Employee Misconduct*, 2001).

Once a finding is reached, the chief of police must notify the subject officer and the complainant. The employee should be advised of the findings and, if sustained, notified that he or she will be disciplined. In all cases, the subject officer should receive a complete copy of the investigative report (*Investigation of Employee Misconduct,* 2001). Similarly, the complainant should receive written notification of the final disposition of the complaint and, at a minimum, the name and contact information of the commanding officer who can answer any questions (Noble and Alpert, 2009).

Self Assessment Exercise

i. What are the principles of an effective complaint process?
ii. Explain the essentials of quality control in any investigatory method

4.0 Conclusion

It is important to conclude here that a strong and effective mechanism is needed and should be present in monitoring and implementing sanity in the way and manner police conduct theri duties so as to maintain and retain the public/community trust on them. This is usually ensured by an instituted internal affairs department. Effective Internal Affairs processes ensure that complaints about an officer are heard and dealt with effectively within the department

5.0 Summary

The discussion was centred basically on the internal mechanism within the police department guiding the Principles of an Effective Complaint and investigation Processes. The unit throws light on Complaint Categories and the general model of the complaint and investigation process using diagrams to illustrate how it works (See figure 1 and 2). The best way investigation report should be filed and presented. In essence, building trust to enhance the image of the police regarding their duties.

6.0 Tutor Marked Assignment

With the aid of a diagram explain both the Complaint and investigation Processes

7.0 References/ Further Reading

Chermak, S. and A. Weiss. *Marketing Community Policing in the News: A Missed Opportunity?* Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, July 2003. www.ncjrs.gov/pdffiles1/nij/200473.pdf

De Angelis, J. and A. Kupchik. *Officer Satisfaction with the Denver Police Complaint Process: A Comparison of the Baseline and Post-Implementation Surveys*. Conducted for the Office of the Independent Monitor, Denver,

Colorado: 2007.
www.denvergov.org/Portals/374/documents/OfficerSatisfaction2006.pdf

Fields, C. *1999–2006 Award-Winning Community Policing Strategies; A Report for the International Association of Chiefs of Police, Community Policing Committee*. Washington,
D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2007.
www.cops.usdoj.gov/files/RIC/Publications/e08071596.pdf

Fisher-Stewart, G. *Community Policing Explained: A Guide for Local Government.*
Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services and International City/County Management Association, 2007.
www.cops.usdoj.gov/files/RIC/Publications/cp_explained.pdf

Hackman, M. J. *Citizen Complaints About Police Use of Force: Bureau Justice of Statistics*
Special Report. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs,
2006. www.ojp.gov/bjs/pub/pdf/ccpuf.pdf

"Investigation of Employee Misconduct: Concepts and Issues Paper." International
Association of Chiefs of Police, National Law Enforcement Policy Center, Alexandria,
Virginia: 2007.

Kelly, S. "Internal Affairs: Issues for Small Police Departments." *FBI Law Enforcement*
Bulletin, vol. 72, no. 7, July 2003, pages 1–6.
www.fbi.gov/publications/leb/2003/july03leb.pdf

Martinelli, T. J. and J. A. Schafer. "First-Line Supervisor's Perceptions of Police Integrity: The Measurement of Police Integrity Revisited," vol. 31 no. 2, 2008, pages 306–323. Bingley, United Kingdom: Emerald Group Publishing Limited.

Nickels, E. L. and A. Verma. "Dimensions of Police Culture Police Culture: A study in
Canada, India, and Japan," vol. 31 no. 2, 2008, pages 186-209. Bingley, United Kingdom:
Emerald Group Publishing Limited.

Noble, J. J. and G. P Alpert. *Managing Accountability Systems for Police Conduct: Internal Affairs and External Oversight.* Prospect Heights, Illinois: Waveland Press, 2009.

Walker, S., S.O. Milligan, and A. Berke. *Strategies for Intervening with Officers through Early Intervention Systems: A Guide for Front-line Supervisors*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, Police Executive Research Forum, February 2006. www.cops.usdoj.gov/files/RIC/Publications/e01060004.pdf

www.discoverpolicing.org:.*A Leadership Guide for State, Local, and Tribal Law Enforcement*

Reiter, L. *Law Enforcement Administrative Investigations: A Supervisory and Agency Guide*
to: Handle Citizen Complaints of Misconduct, Conduct Administrative Investigations, Manage the Internal Affairs Function, and Create Reasonable and Defensible Discipline 2nd Edition. Tallahassee, Florida: Lou Reiter and Associates, 2004.

Thurnauer, B. *Best Practice Guide, Internal Affairs: A Strategy for Smaller Departments*.
Alexandria, Virginia: International Association of Chiefs of Police, 2002.
www.theiacp.org/LinkClick.aspx?fileticket=4B%2f4SDZtgV8%3d&tabid=392

U.S. Department of Justice, Office of Community Oriented Policing Services and Office of
Justice Programs, National Institute of Justice. *Police Integrity – Public Service with Honor,*
A Partnership Between the National Institute of Justice and the Office of Community riented
Policing Services. Washington, D.C., January 1997.
www.ncjrs.gov/pdffiles/163811.pdf

Fisher-Stewart, G. *Community Policing Explained: A Guide for Local Government.*
Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing
Services and International City/County Management Association, 2007.
www.cops.usdoj.gov/files/RIC/Publications/cp_explained.pdf

Hackman, M. J. *Citizen Complaints About Police Use of Force: Bureau Justice of Statistics*
Special Report. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs,

2006. www.ojp.gov/bjs/pub/pdf/ccpuf.pdf

“Investigation of Employee Misconduct: Concepts and Issues Paper.” International
Association of Chiefs of Police, National Law Enforcement Policy Center, Alexandria,
Virginia: 2007.

UNIT 12
SECURITY AND ECOLOGY IN THE AGE OF GLOBALIZATION

1.0 INTRODUCTION

Many situations with a vaguely environmental designation now apparently endanger modern modes of life in the North (as the affluent industrialized parts of the world are now often called). Growing population pressures and environmental crises in the South—the poor and underdeveloped parts of the planet—have long concerned policymakers and academics. Many states have developed security and intelligence agencies, environmental ministries, and international treaty obligations that address population and environmental dynamics. Weather forecasts for many areas now include routine updates of ozone-depletion levels and the variable daily dangers of exposure to ultraviolet radiation. Some discussions address pollution as a technical matter and such phenomena as ozone holes in terms of risks or hazards rather than as security concerns. But since these matters are now also part of international political discourse and policy initiatives, environment cannot be separated from matters of what is now called "global" security. Environmental change and resource shortages are integral to these discussions, which have also taken place against a backdrop of important questions within the North-South political dialogue. In 1992, the largest summit of world leaders took place in Rio de Janeiro to deal with issues of environment and development. Although the level of high political attention to these issues does fluctuate, the global environment has clearly become a matter of continuing international political concern. Some alarmist accounts have even suggested that future security threats to the affluent North will come about because environmental degradation will lead to starvation and the collapse of societies in the South, leading in turn to a massive migration of "environmental refugees."

2.0 Objectives

It is expected that students comprehend

1. **The nature of vulnerabilities and security challenges**
2. **Conflicts arising from environmental and climate changes.**

3.0 Main Body

In 1994, Robert Kaplan garnered much attention in Washington and elsewhere with his alarming predictions of a "coming anarchy" premised on the assumption of resource shortages (Kaplan, 2000). Kaplan suggested that these

resource shortages would occur in part because global population would grow faster than the ability of agriculture to support it (a traditional Malthusian argument). But Kaplan's argument also fits into larger recent arguments about how resource shortages in general cause conflict—the so-called "neo-Malthusian" arguments that underlie a substantial part of environmental-security literature. The 1990s spawned two major interconnected discussions among Northern scholars on these themes.

The first discussion centred on security—its definition and how it might be redefined after the Cold War. This debate included dialogue on which other threats (apart from those related to warfare) ought to be included in comprehensive definitions and policies; it also examined who and what was being secured in the process (Buzan, Wæver, & deWilde, 1998). The redefinition of security has prominently featured environmental considerations (Deudney & Matthew, 1999). Second, a more empirical discussion looked at the narrower question of whether environmental change actually threatened (or could plausibly threaten) security for states in general and the North in particular (Diehl & Gleditsch, 2001). By the end of the 1990s, as the lengthy bibliographies in previous editions of *ECSP Report* attest, the results of this substantial body of empirical research work were appearing in print. Some researchers argue that the environment security debate has evolved in three stages (Rønnfeldt, 1997). First came the initial conceptual work that called for a broader understanding of security than that which dominated Cold War discourses. Second, theorists attempted to sketch out how to specify links between environment and insecurity in order to establish a practical research agenda for scholarly analysis.

The third stage has featured a search for empirical verification or refutation of the initial postulates. While studies are still in progress, enough detailed field work had been done by 2000 to give at least a broad outline of the likely relationships between environment and security and to dismiss definitively much of the early alarmism about international conflict in the form of "ecowars." It is now time to feed these conclusions back into the larger conceptual discussion that first set the field's empirical research in motion. With the wisdom of a decade's research to draw on, environmental security discussions can now move to a fourth stage of synthesis and reconceptualization (Dalby, 2002). In addition to this fourth stage, scholars and policymakers now have to consider current research on biospheric systems and what is now called global change science in their effort to think clearly about both environment and security. Considering matters in these terms adds some crucial dimensions that the 1990s alarmist accounts of neo-Malthusian scarcities left out. Policymakers need to carefully consider both the context of security discussions as well as what their policymaking aims to secure; neither is as obvious as is frequently assumed. In particular, taking ecology ser iously requires questioning more than a few conventional assumptions.

3.1 Environment and Conflict

With these caveats in mind, the development of environmental conflict research through the 1990s can be briefly summarized as six interconnected approaches. First, the Toronto school—as the research groups collectively lead by the University of Toronto's Thomas Homer-Dixon came to be called—emphasizes the construction of scarcity by complex social and environmental processes that in some circumstances also lead to political instability (Homer-Dixon & Blitt, 1998; Homer-Dixon, 1999). The Toronto school argues that simple scarcity as a result of environmental change and population growth is only part of a much more complex situation in which social factors intersect with natural phenomena. These researchers emphasize situations in which elites extend their control over productive resources (in a process called "resource capture") and displace peasants and subsistence farmers ("ecological marginalization"). Resource capture and ecological marginalization, argues the Toronto school, may lead to conflict (as people resist displacement) and environmental damage (as these displaced people are forced to migrate to cities or to eke out their livings by clearing marginal land). In some cases, this process may be connected to state failure and political violence, especially in those developing states in which insurgencies feed on grievances related to injustice and inequity. Identifying where social breakdown and violence occur depends on understanding states' ability to respond to such processes. In Homer-Dixon's analyses, declining state capacity relates in at least four ways to increasing environmental scarcity. First, environmental scarcity increases financial demands on the state for infrastructure. Second, the state faces demands by elites for financial assistance or legal changes for their direct benefit. Third, this predatory elite behaviour may lead to defensive reactions by weaker groups—whether in the form of opposition to legal changes that alter property ownership arrangements or as direct protests against infrastructure "developments" that dispossess the poor. Finally, the general reduction in economic activity caused by the combination of these dynamics can reduce state revenue and fiscal flexibility, further aggravating difficulties. None of the Toronto research suggests that interstate war is likely as a direct consequence of environmental scarcity, although the indirect consequences of social friction caused by large-scale migration—in part across national boundaries—has in some cases caused international elites may aggravate traditional conflicts over land and other resources, especially when these resources are in short supply. Kahl's reading reinforces the ENCOP point that at least a substantial part of rural violence may have its roots in urban politics. A foreign-aid policy of building state capacity in such circumstances may only worsen these situations. In the late 1990s, NATO researchers took on the relationships between environment and security by drawing on the findings of both the Toronto group and ENCOP and adding insights from contemporary tensions. Frequent alarmist newspaper headlines notwithstanding, water wars are also unlikely; the circumstances that would motivate such wars are rare (Lonergan, 2001).

The second approach, embodied in the Environment and Conflicts Project (ENCOP) led by Günther Baechler, links environmental concerns more directly to development and social change in the South (Baechler, 1998). ENCOP examined many different case studies and concluded that, while conflict and environmental change are related in many ways, conflict is more likely to be linked directly to the disruptions of modernity. In summarizing and clarifying the overall ENCOP model, Baechler (1999) stresses that violence was likely to occur in more remote areas, mountain locations, and grasslands— places where environmental stresses coincide with political tensions and unjust access to resources. For ENCOP, the concept of "environmental discrimination" (which emphasizes situations in which politics creates inequitable access to natural resources) connects directly to what Baechler calls a condition of "mal-development." ENCOP links mal-development to a society's transition from subsistence to market economy. In many cases, ENCOP argues, violence occurs as people resist expropriation of resources and the environmental damage caused by development projects. For example, in Bougainville, Papau New Guinea, a long standing and violent insurgency has been directly linked to opposition to a giant mine (Böge, 1999). Colin Kahl's (1998) research tackles these matters in a slightly different but loosely parallel way. Drawing on a detailed analysis of Kenya, Kahl shows how threatened urban German work on climate change and related matters (Carius & Lietzmann, 1999, Lietzmann & Vest, 1999). In this third environmental security approach, these NATO researchers suggest that environmental matters can be understood as a complex series of syndromes, some of which might cause conflict. The comprehensiveness of these syndromes clearly suggests that the notion of environment as a causal factor in conflict is simply too broad to serve as a useful analytical category. But the NATO work also suggests that the environment is an important factor in contemporary social change.

NATO has also sponsored high-profile workshops to encourage dialogues on these themes with Eastern Europe and the post-Soviet states; the proceedings suggest numerous possible ways of thinking about these issues (Lonergan, 1999; Petzold- Bradley et al., 2001).

A fourth school of thinking, linked to the International Peace Research Institute, Oslo (PRIO), has turned the environmental scarcity-conflict argument on its head by suggesting that violence over resources in the South occurs in the struggle to control *abundant* resources (de Soysa, 2000). This research incorporates some economists' discussions about development difficulties in resource-rich areas; it suggests that many wars concern control over revenue streams from resources that have substantial market value. (Examples include timber in Burma, diamonds in Sierra Leone, or oil fields in the Middle East.) The PRIO research directly links violence in some cases to the core-periphery disruptions of native peoples noted by ENCOP. A number of recent studies have reinforced the PRIO argument by tracing the violence surrounding resources directly to larger patterns of global political economy. These studies

sometimes sharply criticize the “neo-Malthusian” tendencies of the Toronto school, which focus on shortages of resources that are supposedly both common and linked to conflict (Peluso & Watts, 2001). Conflict over abundant resources frequently causes environmental disputes, but environmental change is not a simple cause of conflict in these cases. However, resources have become part of the “new wars”1 in the South (Kaldor, 1999). The control of resource exports is now part of a complicated political economy of violence that links identity struggles to (a) international business connections that supply weapons to the protagonists, and (b) the absence of effective state structures. These patterns are frequently complex and not simply matters of greed-driven conflict. Both the international economy as well as political connections to diasporic communities (such as the Tamils in Toronto or the Irish in New York) are factors in these patterns of violence and the role of international organizations in quelling it (Le Billon, 2001).

Michael Klare (2001) has subsequently linked these concerns over resource control and conflict back to older arguments about “resource wars,” in particular to discussions of conflict over global oil supplies. Klare’s argument (the fifth approach) reprises classic geopolitics and reproduces neo-Malthusian narratives of forthcoming stresses and strains in the international system due to decreasing supplies of petroleum. He also suggests that water shortages might create similar dynamics, and he revisits classic concerns about Egypt, Sudan, and Ethiopia fighting over the Nile River waters upon which Egypt’s agriculture and industry depend. Klare’s analysis reiterates the findings of most environment and security literature, suggesting a greater likelihood of violence and conflict related to environment and resources in the South rather than in the affluent North. But as with most of his predecessors, he fails to question the Northern resource-consumption patterns that lead to these difficulties. Klare also fails to seriously consider the possible climate disruptions in the medium-term future if unrestricted carbon-fuel consumption continues. In this vein, a sixth approach is relevant—an approach summarized in the term Global Environmental Change and Human Security (GECHS). These studies examine vulnerabilities of populations to changing environments—specifically, disruptions such as those caused by climate change. GECHS-style research also addresses the welfare and survival of people rather than states (Matthew, 2001). This focus overlaps in part with ENCOP’s research into why the incidence of violence correlates highly with those geographic regions that earn the lowest scores on the UN human-development indices. GECHS research emphasizes how important it is to understand the complexity of both environmental and social processes in specific contexts. It also stresses the obvious point that the rural poor frequently suffer the most vulnerability to both environmental change and the disruptions caused by political violence (Renner, 1996). Human insecurity is very context-dependent, and research and policy alike have to recognize this complexity.

Self Assessment Exercise
Examine the concepts of Security, in relation to violence, environmental change and modernity.

4.0 Conclusion

This paper seek to explain the interconnections between the environment and conflict as many and complex, however it states that the likelihood of large-scale warfare over renewable resources is small. Nonetheless, environmental difficulties do render many people insecure.

5.0 Summary

A parallel conceptual discussion suggests that the empirical work of environmental security research needs to be placed in the larger context of global economic changes and large-scale urbanization of a growing humanity. This urban population increasingly draws resources from rural areas, disrupting indigenous populations. All these dynamics are also complicated by the rapidly increasing scale of human activities, which has induced a level of material- and energy-flow through the global economy that is a new and substantial ecological factor in the biosphere. Given the scale of these processes, societies should carefully consider these interconnections and reduce their total resource throughput to improve environmental security and develop sustainable modes of living for the future. This summary will be clearly understood in the subsequent unit.

6.0 Tutor Marked Assignment

Discuss the control of resource exports as a complicated political economy of violence

7.0 References/ Further Reading

Baechler, Günther. (1999). *Violence through environmental discrimination: Causes, Rwanda arena, and conflict model*. Dordrecht: Kluwer Academic Publishers.

Böge, Volker. (1999). “Mining, environmental degradation and war: The Bougainville case.” In Mohamed Suliman (Ed.), *Ecology, politics and violent conflict* (pages 211-227). London: Zed Books.

Buzan, Barry; Wæver, Ole; & de Wilde, Jaap. (1998). *Security: A new framework for analysis*. Boulder: Lynne Rienner.

Carius, Alexander & Lietzmann, Kurt M. (Eds.). (1999). *Environmental change and security: A European perspective*. Berlin: Springer.

de Soysa, Indra. (2000). “The resource curse: Are civil wars driven by rapacity or paucity?” In Mats Berdal and David M. Malone (Eds.), *Greed and*

grievance: Economic agendas in civil wars (pages 113-135). Boulder: Lynne Rienner.

Deudney, Daniel & Matthew, Richard. (Eds.). (1999). *Contested grounds: Security and conflict in the new environmental politics*. Albany: State University of New York Press.

Diehl, Paul & Gleditsch, Nils Petter. (Eds.). (2001). *Environmental conflict*. Boulder: Westview.

Kaldor, Mary. (1999). *New and old wars*. Stanford: Stanford University Press.

Kaplan, Robert. (2000). *The coming anarchy: Shattering the dreams of the post cold war*. New York: Random House.

Klare, Michael. (2001). *Resource wars: The new landscape of global conflict*. New York: Metropolitan Books.

LeBillon, P. (2001). "The political ecology of war: Natural resources and armed conflicts." *Political Geography 20*(5), 561-584.

Lietzmann Kurt M. & Vest, Gary D. (Eds.). (1999). *Environment and security in an international context*. (Committee on the Challenges of Modern Society, Report No. 232). Bonn: North Atlantic Treaty Organization.
Lonergan, Steve C. (Ed.). (1999). *Environmental change, adaptation and security*. Dordrecht: Kluwer Academic Publishers.

Petzold-Bradley, Ellen; Carius, Alexander; & Vincze, Arpod (Eds.). (2001). *Responding to environmental conflicts: Implications for theory and practice*. Dordrecht: Kluwer Academic Publishers.

Renner, M. (1996). *Fighting for survival: Environmental decline, social conflict and the new age of insecurity*. New York: Norton.

Rønnfeldt, Carsten F. (1997). "Three generations of environment and security research." *Journal of Peace Research 34*(4), 473- 482.

Matthew, Richard. (2001). "Environmental stress and human security in Northern Pakistan." *Environmental Change and Security Project Report 7*, 17-31.

Peluso, Nancy & Watts, Michael (Eds.). (2001). *Violent environments*. Ithaca: Cornell University Press.

UNIT 13

SECURITY AND ECOLOGY IN THE AGE OF GLOBALIZATION II

1.0 INTRODUCTION

Empirical research into the *Contexts of Human Security*, environment and conflict has generated considerable insight into the practices of violence; it has also made very clear that research results are in part determined by how questions are formulated. But these advances must then be connected back into the larger debate about security that has been in play in the North since the end of the Cold War—a debate that has explored environmental themes as part of an emphasis on the security of people, not states. The highest profile articulation of "human security" comes from the United Nations Development Program (UNDP) in its *Human Development Report 1994* (UNDP, 1994). These discussions have dusted off and reintegrated themes of poverty and misery that had been important in the early days of the United Nations but which had been swept aside during the Cold War.

2.0 OBJECTIVES

At the end of this unit, students should be able to:

1. Understand the global approach to security
2. Highlight Current trend in environmental security debates

3.0 MAIN BODY

The *Human Development Report 1994* includes environmental factors as one of its human security themes. In its discussion of global threats to human security (dangers caused by the actions of millions of people rather than the deliberate aggression of specific states), the *Report*'s use of "environment" generally refers to threats such as trans-boundary air pollution, CFCs and ozone depletion, greenhouse gases and climate changes, biological-diversity reduction, coastal marine pollution, and global fish-catch reductions. The *Report* clearly suggests that environmental threats to human security are best dealt with by preventive and anticipatory action rather than crisis intervention.

But the *Report*'s assumption of a universal humanity that faces common challenges in a world of huge inequities and political violence has limitations as well as consequences for discussions of sustainable development. The greatest enthusiasm for global approaches to security comes from North America and European states, which are least likely to face direct military confrontation (Stares, 1998). Is the locus of both this enthusiasm and the environmental security debates noted above politically insignificant (Barnett, 2000)? Current consumption patterns threaten the South because of (a) the North's extensive consumption of resources, and (b) the ecological and social disruptions caused in many rural areas of the South by that resource extraction (Redclift, 1996). While this pattern is not the sole cause of Southern insecurity, it plays an important role overlooked in the neo-Malthusian specifications of conflict caused by resource shortages. If the North merely seeks to maintain its overall pattern of resource consumption within limits that will not disrupt Northern prosperity, merely reformulating the concept of human security will continue to compromise the real security of Southern populations. The case of greenhouse gases and multilateral environmental agreements (such as the Kyoto Protocol) makes clear the link between consumption and security (Adams, 2000). Intensive resource use (particularly of fossil fuels) has powered the development of the industrialized world. Not surprisingly, states that have begun to develop more recently balk at forgoing such heavy resource use. U.S. negotiating positions have also frequently been hampered by the common U.S. stand that all states must agree on international arrangements before the United States can support a regime for greenhouse gas limitations. Widely varying national economic situations, however, have made establishing common standards for such an agreement difficult. Meanwhile, the overall focus on emissions limits and regulations continues to foreclose opportunities for technological innovation by focusing once again on end-of-the-pipe thinking rather than on ways to rebuild economies that reduce resource throughputs. The geographic messiness of the global economy—which is marked by resource extraction from the South and export to the North (Grove, 1997)—complicates formulating a treaty on greenhouse gas emissions. Does gas flared off a well in Nigeria count against Nigeria when Europe uses the oil to fuel its cars? Does a Russian forest that absorbs carbon dioxide count as a national or a global carbon "sink"? In addition, the establishment of "emissions" and "sinks" as tradable items further complicates this geography. Rich countries can buy sinks in poor countries to offset their carbon dioxide production—allowing the wealthy to forgo reductions of greenhouse emissions. While such mechanisms may be of use for some economic policies, they might also allow policymakers to avoid the crucial issue of reducing total carbon dioxide levels in the atmosphere. One can also easily envision scenarios in which governments implement international agreements concerning sinks with disregard for traditional access to forests or the use of forests for survival by the poor and marginal—precisely those who are most insecure. From Bougainville (Böge, 1999) to Burma (Talbott & Brown, 1998), marginal peoples suffer from dispossession, violence, and the expropriation of resources to feed international

markets. Elsewhere, the poor are forced off subsistence plots to make way for expanding commercial agriculture or large infrastructure projects such as highways and dams. Arguments about intellectual property rights, control over ancestral territories, traditional seed varieties, and medicinal plants are all part of the commercial expansion that lies at the heart of most development projects (Miller, 2001). In addition, as noted above, displaced people become migrants, often landing in burgeoning Southern cities where they, too, become part of the urban economy that the expanding commercial agriculture sector must feed. In the process, these growing numbers of urban consumers make ever-larger demands on the surrounding countryside to supply the food and other commodities they use. In short, there is a large-scale geographic dimension to what Karl Polanyi (1957) called "the great transformation" to commercial society. The 20th century was undoubtedly the century of urbanization, powered by rural-urban migration; and this crucial transformation (with all its environmental and social consequences) frequently gets lost, both in many economic specifications of state "development" and in discussions of scarcity-induced violence.

3.1 Environment and Ecology

But the category of "environment" itself is not always useful in these discussions. While environment is at once an unavoidable general category of great importance, it also needs to be broken down into subcategories if useful, practical research is to be carried out. Indeed, "environment" (traditionally understood as the backdrop for human activity) is no longer very helpful in formulating policy options within the biosphere. On the other hand, the global economy's various environmental disruptions are as a whole the most worrisome dynamic for human security in many places. Such nuances are of fundamental importance for analysis and policymaking. For the question of how environment and conflict interact, even a narrower focus on renewable resources or pollution does not produce clearly defined analytical categories. River-water supplies, soil moisture levels, or deforestation rates are much more useful indicators of specific factors that might influence conflict or its absence. Nonetheless, health issues connected to pollution clearly do matter politically, as elites in the former Soviet bloc and elsewhere have discovered from the 1980s on. But the case of the Aral Sea—whose disappearance (an indirect result of industrial agriculture) is leading to a loss of livelihood and significant related health impacts—does not confirm the simple behaviourist assumption that such assaults on health or well-being will cause people to flee or fight. Poverty, state restrictions on migration, and numerous social and cultural factors complicate matters. Combining such diverse phenomena as climate change, toxic industrial pollution, soil erosion, deforestation, aquifer depletion, and shortages of subsistence farmland into the category of "environment" is also frequently not helpful. These phenomena relate to a variety of human societies in such numerous ways that generalized concepts can rarely make useful contributions to their analysis.

Researchers interested in conflict have divided environmental themes into many more specific targets of investigation, such as water, forests, and other resources. Researchers have also started to look at individual resources in particular places. In addition, there is no consensus definition of environmental insecurity (Barnett & Dovers, 2001). The assumption that the environment is separate from both humanity and economic systems lies at the heart of the policy difficulties facing sustainable development and security thinking. The idea of environment as an independent variable—something that is beyond human control and that stresses human societies in ways that require a policy response— presents a problem for the environmental dimension of human security. As the burgeoning environmental history literature has now made abundantly clear, the sheer scale of human activity renders this assumption inadequate for both scholarship and policy formulation (McNeill, 2000). Instead, researchers and decision-makers should focus more specifically on *ecology*. Ecology studies the flows of energy and food through complex systems made up of living things, air, water, and soil. Human activity is now a major part of these flows; and the disruptive impacts of humanity are not simply a matter of climate change but rather a matter of numerous and simultaneous changes to many natural systems. We are literally remaking the biosphere—indirectly by changing the air that we breathe, and directly by disrupting forests and grasslands through mining, agriculture, deforestation, and urbanization. The scale of this transformation requires us to understand humanity as a major force remaking the planetary ecosystem (IGBP, 2001). Environment is no longer simply the backdrop to human activities: it is increasingly the *human-made context* for our lives.

Policy that usefully addresses both sustainability and security has to start from these scientific insights— even if our conventional categories for managing human societies do not easily fit with these new understandings. Ecology should not be restricted to a matter of environmental politics among nation-states (Litfin, 1998). Contemporary research shows that the flows of resources and materials that support the global economy are causing most environmental change. From shrimp to oil to timber and coffee, Northern consumption is supplied by resources from all over the world with unavoidable environmental consequences (Redclift, 1996). These consequences, however, are often obscured from Northern consumers who buy the commodities that the global economy apparently miraculously and mysteriously supplies.

3.2 A Conceptual Synthesis?

The preceding discussion outlines the global interconnections that environmental security research now struggles to incorporate into both academic analysis and policy advice. Putting all of this discussion's elements into one simple overview is a conceptually risky business. But the following sketch—and it is no more than a sketch—suggests how all of these pieces can form a fairly simple scheme that allows us to clarify the dilemmas of human security and to factor the appropriate contexts into policy advice.

First, we must recognize that rich and powerful urban elites have both (a) a disproportionate impact on the earth's natural systems, and (b) also make many of the policy decisions regarding resource-use and pollution. Second, global population is growing; and more importantly, it is becoming urbanized. As a result, this population increasingly depends on resources and food supplies from rural areas that are sometimes remote. Third, this process is happening in the context of rapid globalization—with its inherent dislocations— of an economy ever more dependent on petroleum products. Fourth, nation-states (even well-functioning ones) are frequently not the appropriate political entities to make decisions about many economic and environmental matters that flow across their borders in a highly uneven global economy. Extrapolating from the work of some Indian scholars to the global scale allows us to put these elements into a single summary conceptual scheme. In considering the state of Indian society in the 1990s, Madrav Gadgil and Ramachandra Guha (1995) classified people in terms of their ecological situation by using three catergories. First, Gadgil and Guha termed as "ecosystem people" those locally-based populations who use their own labor to survive by cultivating and harvesting food and other resources from specific localities. Second, many of these people have been displaced from their homes in recent decades, becoming "ecological refugees."

Finally, these ecological refugees often gravitate to rapidly expanding urban centers, where they become "omnivores"— those who literally eat everything, often foods and other resources brought from great distances to the metropoles. Many omnivores in developed countries may also live or spend a substantial part of their lives in rural areas; but their economic support system is dependent on flows of resources from a distance. These categories are obviously not mutually exclusive: many people have the characteristics of more than one category. For example, suburban dwellers growing vegetables for their family's use are in that sense analogous to ecosystem people, and most ecosystem people are involved in at least a few commercial transactions for luxury goods. But Gadgil and Guha's categorical scheme has the advantage of specifying people in terms of their functional position in both ecosystems and (more generally) within the biosphere. Their labels also challenge us to think about our own ecological situations. Most of the people who read policy discussions of environmental security are likely to be omnivores. And the processes of extracting the resources that support their lives—be those resources oil from Ogoni-land in Nigeria, diamonds from Sierra Leone, or tropical timber from Angola— may be the cause of considerable disruption and violence (Le Billon, 2001). The ecological-situation framework suggests that disruptions caused by the spread of the market system—which demands transfers of ever-larger supplies from rural areas to cities for omnivore consumption—perpetually threaten to turn ecosystem people into ecological refugees. When serious environmental disruptions occur (including droughts, storms, and floods), ecosystem people often become impoverished ecological refugees, while

omnivores have the economic flexibility to simply buy their foods and resources from elsewhere. This crucial geography also relates to the overall vulnerability of the poor and marginal in many places. Ecosystem people often have substantial survival mechanisms—but these mechanisms are sometimes tragically overwhelmed by expansions of the market economy that reduce access to traditional food supplies and storage. The curtailment of forest access, the enclosure of common-grazing lands, and the diversion of water into irrigation schemes all disrupt access to traditional food supplies. Traditional non-commercial methods of food storage are also often superceded by modern commercial arrangements. In good times, farmers are happy to sell their crops rather than store them, but when disaster strikes, the poor often lack the means to buy suddenly scarce foods. Each of the three ecological-situation categories obviously entails very different human consequences and perspectives on the process. But policymakers who address sustainable development must bear in mind that they nearly always come to the negotiating table as omnivores, and as such they bring developed economy and urban assumptions to bear on problems that are at odds with rural societies. Urban definitions of sustainable development are frequently less than helpful, especially when urban aesthetic criteria view the environment as something pristine that needs "protection" from rural inhabitants. Such mindsets frequently fail to recognize the complexity of rural social arrangements or the ecological contexts of local residents. And these difficulties are compounded by urban stereotypes of peasants as backward and incapable of using resources "rationally"— i.e., in a short-term, commercial way (Scott, 1998). In the hands of journalists like Kaplan (1994, 2000), these arguments are all too frequently extended to suggest that rural populations are the source of numerous security threats to Northern omnivores.

3.3 Policy Implications

In his recent book *The Ingenuity Gap*, Homer- Dixon (2000) tries to escape the intellectual limitations of thinking about these matters within conventional international relations formulations. Homer-Dixon notes the repeated collapse of environmental security discussions into debates between optimists and pessimists, cornucopians and neo-Malthusians; and he recognizes the pointlessness of these oppositions for both the environment and policy advice. Instead, his recent focus on the "ingenuity gap" in both developed and developing countries suggests that the largest problems humanity faces are those related to our frequent inability to think creatively and in a timely and contextualized manner. Homer-Dixon argues that we need to frame policy problems so that proposed solutions emphasize adaptability and social as well as technical innovation. And he concludes that environment in terms of security—or environment as a simple cause of conflict—are inadequate frameworks for the task at hand. Homer-Dixon himself has applied ingenuity to think anew about development and environment in ways that practically tackle human difficulties while being sensitive to local circumstances as well as the

growing interconnections of the global economy. Likewise, Baechler (1999) insists that questions of vulnerability and security must be considered together. He also argues that innovation and conflict-resolution require both detailed political work and the provision of options to marginalized populations. But his analysis does not conclude that solutions will necessarily come from increased state capacity. Indeed, in quite a number of the cases that Baechler has analyzed, the zealous attempts of states to remake their rural areas in the process of development has aggravated conflict rather than facilitated useful social innovation. This realization is an important corrective to the simple assumption that further modernization and development is the
answer. In stark contrast, Klare (2001) points to the dangers of war over resources, but he offers few political ideas for escaping from this potential mess. Helping marginal populations adapt to environmental change will require political ingenuity. Large measures of ingenuity will also be required to reduce unsustainable elite consumption as well as to formulate wise policies that constrain how resource extraction, pollution, and atmospheric change disrupt rural ecologies. Above all, we should prioritize the kind of technologies and structures that will minimize resource use in the medium- and long-term future over "end-of-thepipe" regulations that focus on emissions. How the Wuppertal Institute in Germany formulates these terms is especially suggestive (Sachs, Loske, & Linz, 1998). Wuppertal researchers point to the distant Southern consequences of Northern consumption—such as mining wastes, deforestation, and displaced peasant farmers—as the key to global sustainable development. Reducing the total material throughput in the economy, they argue, is the key to (a) reducing total ecological damage, while simultaneously (b) supporting economically benign modes of trade that will improve the prospects for the poorest Southern populations. Poverty reduction thus depends on restricting those exports that have caused the worst environmental destruction. Solar and wind energy are perhaps best emblematic of recent innovative suggestions that emphasize how ecological flows connect with human security. Once produced and installed, these technologies minimize the flow of material through ecosystems. Wind and sun provide the energy. No fuels have to be transported. No pollution alters the atmosphere. They can be installed close to where power is needed, thus reducing the materials needed to move energy. Consumers get electricity and warm water, but do so without importing oil from distant lands in a process that frequently disrupts local ecologies and social systems. When combined with intelligent building design that minimizes energy requirements, solar and wind energy offer tremendous potential for practical reductions in greenhouse gas emissions. Smart buildings and appropriate architecture can, when designed carefully, both reduce energy costs and pollution as well as provide comfortable working environments that enhance productivity. But these technical difficulties seem trivial in comparison to the political and administrative hurdles that face ecologically friendly design, as the great difficulties that face innovative urban architects in many countries attest (Brugman, 2001). To create sustainable communities—communities that do not environmentally harm distant places—policy innovation must extend to local

governments and building codes. A sustainable-development policy that also attempts to enhance human security demands innovative design and policies to minimize the ecological impact of new buildings and transportation systems. These areas are not where most security analysts focus their attention when thinking about environment, but such ingenuity will have large human security payoffs for many people.

3.4 Rethinking Ecology and Security

Northern consumption, its consequences for Southern human security, and the shift in focus from environment to ecology are now fundamental to rethinking environmental security. The cumulative results of omniverous consumption are literally remaking parts of the global biosphere in ways that might cause all sorts of unforeseen disruptions. Ecological systems are already adapting to the rise in global temperature in the last few decades; and they are doing so in ways that are site-specific (Walther et al., 2002). While omnivores are in part protected from these disruptions by their abilities to use purchasing power in the global economy to switch supply sources, ecosystem people frequently do not have that option. Many more of them may be turned into environmental refugees in the coming decades—not because of any local shortages of resources, but as a consequence of the disruptions caused both directly and indirectly by omniverous consumption. Environmental security thinking must focus explicitly on these ecological interconnections as a key component of both (a) environmental disruptions, and (b) wars over control of resource exports. Indeed, environmental security needs to take ecology much more seriously. While nation-states may provide administrative and legal structures within which policy is formulated and administered, such spatial categories do not even come close to capturing the flows of energy and materials through our lives.

Self Assessment Exercise

How does global population increase contribute to security threat?

.

4.0 Conclusion

Ecologically understanding security as the assurance of relatively undisturbed ecological systems in all parts of the biosphere—requires that researchers and policymakers (a) even more drastically reframe conventional categories of security, and (b) integrate the question of whom is secured into their analyses. Only then can the contexts of environmental insecurity be treated with the seriousness they deserve.

5.0 Summary

This section highlights the *Human Development Report 1994 which* includes environmental factors as one of its human security themes. It also emphasises Policy that usefully addresses both sustainability and security from giving scientific insights to understanding conventional categories for managing human societies, global interconnections, environmental security and research

that incorporate both academic analysis and policy advice in security management.

6.0 Tutor Marked Assignment

The idea of environment as an independent variable—something that is beyond human control and that stresses human societies in ways that require a policy response— presents a problem for the environmental dimension of human security. Discuss

7.0 References/ Further Reading

Baechler, Günther. (1999). *Violence through environmental discrimination: Causes, Rwanda arena, and conflict model*. Dordrecht: Kluwer Academic Publishers.

Barnett, Jon. (2000). "Destabilizing the environment-conflict thesis." *Review of International Studies 26*(2), 271-288.

Barnett, Jon & Dovers, Stephen. (2001). "Environmental security, sustainability and policy." *Pacifica Review 13*(2), 157-169.

Böge, Volker. (1999). "Mining, environmental degradation and war: The Bougainville case." In Mohamed Suliman (Ed.), *Ecology, politics and violent conflict* (pages 211-227). London: Zed Books.

Brugman, Jeb. (2001). "Agenda 21 and the role of local government." In Felix Dodds (Ed.), *Earth summit 2002: A new deal* (pages 40-48). London and Sterling, VA: Earthscan.

Grove, Richard. (1997). *Ecology, climate and empire: Colonialism and global environmental history, 1400-1940*. Cambridge: White Horse.

Homer-Dixon, Thomas. (2000). *The ingenuity gap: How can we solve the problems of the future?* New York: Knopf.

International Geosphere Biosphere Program (IGBP). (2001). *IGBP Science 4*. "Global change and the earth system: A planet under pressure." [On-line] Available: http:// igbp.kva.selluploads/ESO_IGBP4.pdf

Kaplan, Robert. (1994). "The coming anarchy." *The Atlantic Monthly 273*(2), 44-76.

Kaplan, Robert. (2000). *The coming anarchy: Shattering the dreams of the post cold war*. New York: Random House.

Klare, Michael. (2001). *Resource wars: The new landscape of global conflict*. New York: Metropolitan Books.

LeBillon, P. (2001). “The political ecology of war: Natural resources and armed conflicts.” *Political Geography 20*(5), 561-584.

Gadgil, Madrav & Guha, Ramachandra. (1995). *Ecology and equity: The use and abuse of nature in contemporary India*. London: Routledge.

McNeill, John R. (2000). *Something new under the sun: An environmental history of the twentieth-century world*. New York: Norton.

Polanyi, Karl. (1957). *The great transformation*. Boston: Beacon.

Redclift, Michael. (1996). *Wasted: Counting the costs of global consumption*. London: Earthscan.

Sachs, W.; Loske, R.; & Linz, M. (1998). *Greening the north: A post-industrial blueprint for ecology and equity*. London: Zed

Scott, J.C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed*. New Haven: Yale University Press.

Stares, Paul B. (Ed.). (1998). *The new security agenda: A global survey*. Tokyo: Japan Centre for International Exchange.

Walther, Gian-Reto; Post, Eric; Convey, Peter; Menzel, Annette; Parmesani, Camille; Beebee, Trevor J.C.; Fromentin, Jena Marc; Guldburg, Ove Hoegh; & Bairlein, Franz. (2002, 28 March). “Ecological responses to recent climate change.” *Nature 416*, 389-395.

UNIT 14
Information Security: *E-government and Denial of Service (DoS) Attacks.*

1.0 INTRODUCTION

Since we live in a world where electronic and Internet technologies are playing an important role in helping us lead easier lives, local and state governments are required to adopt and participate in this technology revolution. Digital government or e-government technologies and procedures allow local and national governments to disseminate information and provide services to their citizens and organisations in an efficient and convenient way resulting in reducing waiting lines in offices and in minimizing the time to pick up and return forms and process and acquire information. This modernization of government facilitates the connection and cross cooperation of authorities in several levels of government—central, regional, and local—allowing an easy interchange of data and access to databases and resources that would be impossible otherwise. E-government undoubtedly makes citizens' lives and communication easier by saving time, by avoiding and bypassing the bureaucracy, and by cutting down paper work. It also provides the same opportunities for communication with government not only to people in cities but also to people in rural areas. Moreover, e-government permits greater access to information, improves public services, and promotes democratic processes.

2.0 Objectives

This unit examines increasing using of electronic and internet technology in the dissemination of ideas and transaction of governmental activities. It is therefore envisaged that students should be able to comprehend the concept of denial service as a security threat in a globalising world of technology and e-governance.

3.0 Main body

This shift to technology use and the transition to a "paperless government" is constantly increasing. According to Holden, Norris, and Fletcher (2003), in

1995 8.7% of local governments had Web sites, while in 2003 this number showed an increase that reached 83%. Despite these encouraging statistics, the adoption of digital government proceeds with a slow pace as security issues, like confidentiality and reliability, affect the fast progress of e-government. Since e-government is mainly based on Internet technologies, it faces the danger of interconnectivity and the well-documented vulnerabilities of the Internet infrastructure. The Institute for E-Government Competence Centre (IFG.CC, 2002) states that in 2002, 36 government Web sites were victims of intrusions. Most of the e-government attacks have taken place in Asia (25%) and more precisely in China and Singapore (19%), as well as in the USA (19%). According to the U.S. Subcommittee on Oversight and Investigations (2001), the FedCIRC incident records indicate that in 1998 the number of incidents that were reported was 376, affecting 2,732 U.S. Government systems. In 1999, there were 580 incidents causing damage on 1,306,271 U.S. Government systems and in 2000 there were 586 incidents having impact on 575,568 U.S. government systems. Symantec (2004) (Volume VI, released September 2004, activity between January 2004 and June 2004) gives information about Government specific attack data. In this report, one can see that the third most common attack e-government has faced, besides worm-related attacks and the Slammer worm, is the TCP SYN Flood denial of service attack. So in order to have effective e-government services without interruptions in Web access as well as e-mail and database services, there is a need for protection against DoS attacks. Only with reliable e-government services not threatened by DoS attacks governments may gain the trust and confidence of citizens. Moore, Voelker, and Savage (2001) state that the denial of service (DoS) attacks constitute one of the greatest threats in globally connected networks, whose impact has been well demonstrated in the computer network literature and have recently plagued not only government agencies but also well known online companies.

The main aim of DoS is the disruption of services by attempting to limit access to a machine or service. This results in a network incapable of providing normal service either because its bandwidth or its connectivity has been compromised. These attacks achieve their goal by sending at a victim a stream of packets in such a high rate so that the network is rendered unable to provide services to its regular clients. Distributed denial of service (DDoS) is a relatively simple, yet very powerful, technique to attack Internet resources. DDoS attacks add the many-to-one dimension to the DoS problem making the prevention and mitigation of such attacks more difficult and their impact proportionally severe. DDoS attacks are comprised of packet streams from disparate sources. These attacks use many Internet hosts in order to exhaust the resources of the target and cause denial of service to legitimate clients. DoS or DDoS attacks exploit the advantage of varying packet fields in order to avoid being traced back and characterized. The traffic is usually so aggregated that it is difficult to distinguish between legitimate packets and attack packets. More importantly, the attack volume is often larger than the system can handle.

Unless special care is taken, a DDoS victim can suffer damages ranging from system shutdown and file corruption to total or partial loss of services. Extremely sophisticated, "user-friendly," and powerful DDoS toolkits are available to potential attackers increasing the danger that an e-government site becomes a victim in a DoS or a DDoS attack by someone without a detailed knowledge of software and Internet technologies. Most of the DDoS attack tools are very simple and have a small memory size something that is exploited by attackers, who achieve easily implementation and manage to carefully hide the code. Attackers constantly modify their tools to bypass security systems developed by system managers and researchers, who are in a constant alert to modify their approaches in order to combat new attacks. The attackers in order to have more devastating results change their tactics and the way they launch DoS attacks.

One of these tactics is the silent degradation of services for a long period of time in order to exhaust a large amount of bandwidth instead of a quick disruption of network services. The result of these attacks in government organisations among others include reduced or unavailable network connectivity and, consequently, reduction of the organisation's ability to conduct legitimate business on the network for an extended period of time. The duration and the impact of the attack depends on the number of possible attack networks. It is also worth bearing in mind that even if an organisation is not the target of an attack, it may experience increased network latency and packet losses, or possibly a complete outage, as it may be used from the attacker in order to launch a DDoS attack. In this unit, we stress the severity that a DoS attack may have for e-government agencies. To this end, statistics and characteristic incidents of DoS attacks in e-government agencies are presented. Furthermore, we present a classification of DoS and DDoS attacks, so that one can have a good view of the potential problems. Moreover, we outline a list of best practices that can be used in government organisations in order to further strengthen the security of their systems and to help them protect their systems from being a part of a distributed attack or being a target of DoS/DDoS attacks. Long-term countermeasures are also proposed that should be adopted for more efficient solutions to the problem. Following this introduction, this unit is organised as follows. In the section "Denial of Service Attacks" the problem of DoS attacks is investigated, DoS incidents and results from surveys related to DoS attacks, and a classification of DoS attacks are presented. In the section "Distributed Denial of Service Attacks" the problem of DDoS attacks is introduced, giving the basic characteristics of well known DDoS tools, and presenting a taxonomy of DDoS attacks. In the section "Classification of DDoS Defence Mechanisms," we present the DDoS defence problems and propose a classification of DDoS defence mechanisms. In the section "Best Practices for Defeating Denial of Service Attacks" best practices for defeating DoS attacks that can be used by government organizations are presented, while in the section "Long Term Countermeasures" some long-term efforts against DoS attacks are presented.

3.1 DENIAL OF SERVICE ATTACKS

Defining Denial of Service Attacks

The WWW Security FAQ (Stein & Stewart, 2002) states that "a DoS attack can be described as an attack designed to render a computer or network incapable of providing normal services." In a DoS attack, a computer or network resource is blocked or degraded resulting in unavailable system resources but not necessarily in the damage of data. The most common DoS attacks target the computer network's bandwidth or connectivity (Stein & Stewart, 2002). In bandwidth attacks, the network is flooded with a high volume of traffic leading to the exhaustion of all available network resources, so that legitimate user requests cannot get through, resulting in degraded productivity. In connectivity attacks, a computer is flooded with a high volume of connection requests leading to the exhaustion of all available operating system resources, thus rendering the computer unable to process legitimate user requests.

Denial of Service Incidents

Undoubtedly, DoS attacks are a threatening problem for the Internet, causing disastrous financial losses by rendering organisations' sites off-line for a significant amount of time as we can easily confirm by frequent news reports naming as victims of DoS attacks well-known large organisations with significant exposure in the e-economy. Howard (1998) reports denial of service attacks' statistics where one can see the dramatic increase in such attacks even in the first years of the Web. The Internet Worm (Spafford, 1998) was a prominent story in the news because it "DoS-ed" hundreds of machines. But it was in 1999 when a completely new breed of DoS attacks appeared. The so-called distributed denial of service attacks stroke a huge number of prominent Web sites. Criscuolo (2000) reports that the first DDoS attack occurred at the University of Minnesota in August 1999. The attack, flooding the Relay chat server, lasted for two days and it was estimated that at least 214 systems were involved in the attack launch. In February 2000, a series of massive denial-of-service (DoS) attacks rendered out of service several Internet e-commerce sites including Yahoo.com. This attack kept Yahoo off the Internet for 2 hours and lead Yahoo a significant advertising loss. In October 2002 (Fox News, 2002), 13 routers that provide the DNS service to Internet users were victims of a DDoS attack. Although the attack lasted only for an hour, 7 of the 13 root servers were shut down, something that indicates the potential vulnerability of the Internet to DDoS attacks. In January of 2001, Microsoft's (WindowsITPro, 2001) Web sites hosting Hotmail, MSN, Expedia, and other major services were inaccessible for about 22 hours because of a DDoS attack.

Despite attacks on high-profile sites, the majority of the attacks are not well publicized for obvious reasons. CERT (2001) reports that in July 2001, the Whitehouse Web site was the target of the Code Red worm. The attack on the Whitehouse lasted from about 8 a.m. to about 11:15 a.m. Between 1 p.m. and 2 p.m., page request continued failing, while after 2 p.m. the site was

occasionally inaccessible. In order to alleviate the effects of the attack, the Whitehouse momentarily changed the IP address of the Whitehouse.gov Web site. Sophos.com (2002) reports that in June 2002, the Pakistani's Government Web site accepted a DoS attack that was launched by Indian sympathizers. The attack was launched through a widespread Internet worm called W32/Yaha-E, which encouraged Indian hackers and virus writers to launch an attack against Pakistan Government sites. The worm arrived as an e-mail attachment and its subject was relative to love and friendship. The worm highlighted the political tensions between Indian and Pakistan and managed to render the www.pak.gov.pk Web site unreachable. The worm created a file on infected computers that urged others to participate in the attack against the Pakistani government. ITworld.com (2001) reports that even the site of CERT was the victim of a DDoS attack on May 28, 2001. Although the CERT Coordination Center is the first place where someone can find valuable information in order to be prevented against malicious cyber attacks it was knocked offline for two days by a DDoS attack accepting information at rates several hundred times higher than normal. Cs3.Inc (2005) reports that a DDoS attack was launched on the U.S. Pacific command in April 2001. The source addresses of the attack belonged to the People's Republic of China, although the exact origin of the attack has yet not been identified. Despite the fact that the internal networks of the command were not affected, in the long-term no one can deny the fact that critical government operations may be easily disrupted by attackers. After this incident, the political tension between the two countries increased considerably.

The U.S. government worries that U.S. critical network assets may be a target of a DDoS attack as a digital continuation of the terrorist attacks against New York in September of 2001. But government systems can not only be victims of DoS attacks, but may also be used unwittingly in order for a DoS attack to be performed by hosting the agents of a DDoS attack, thus participating involuntarily in the conduction of the attack. Moore et al. (2001) report that in February of 2001, UCSD network researchers from the San Diego Supercomputer Center (SDSC) and the Jacobs School of Engineering analyzed the worldwide pattern of malicious denial-of-service (DoS) attacks against the computers of corporations, universities, and private individuals. They proposed a new technique, called "backscatter analysis" that gives an estimate of worldwide denial of service activity. This research provided the only publicly available data quantifying denial of service activity in the Internet and enabled network engineers to understand the nature of DoS attacks. The researchers used data sets that were collected and analyzed in a three-week long period. They assessed the number, duration, and focus of the attacks, in order to characterize their behaviour and observed that more than 12,000 attacks against more than 5,000 distinct targets, ranging from well-known e-commerce companies to small foreign Internet service providers and even individual personal computers on dial-up connections. Some of the attacks flooded their targets with more than 600,000 messages/packets per second. In addition, they

reported that 50% of the attacks were less than ten minutes in duration, 80% were less than thirty minutes, and 90% lasted less than an hour. Two percent of the attacks were longer than five hours, 1% is greater than ten hours, and a few dozen spanned multiple days.

Furthermore, according to this research, 90% were TCP-based attacks and around 40% reached rates as high as 500 packets per second (pps) or greater. Analyzed attacks peaked at around 500,000 pps, while other anecdotal sources report larger attacks consuming 35 megabits per second (Mbps) for periods of around 72 hours, with high-volume attacks reaching 800 Mbps. The Computer Security Institute (2003) in the 2003 CSI/FBI survey reported that denial of service attacks represent more than a third among the WWW site incidents, where unauthorized access or misuse was conducted. Forty-two percent of respondents to the 2003 survey reported DoS attacks. In 2000, 27% reported such attacks. There appears to be a significant upward trend in DoS attacks. The Computer Security Institute (2004) in the 2004 CSI/FBI survey reported that the highest reported financial losses due to a single DoS attack increased from $1 million in 1998 to $26 million in 2004 and emerged for the first time as the incident type generating the largest total losses. We should also keep in mind that many government organisations interpret DDoS attacks as simply being an experience of inadequate service from their ISP and are not aware that they are under attack. This has as result the fact that nine out of ten DDoS attacks go unreported. In spite of such evidence, most government organisations overlook the necessity of using preventive mechanisms to combat DoS attacks. Although there is no panacea for all types of DoS attacks, there are many defence mechanisms that can be used in order to make the launch of an attack more difficult and provide the means to reach the disclosure of the identity of the attacker.

3.2 Denial Of Service Attack Classification

DoS attacks can be classified into five categories based on the attacked protocol level. More specifically, Karig and Lee (2001) divide DoS attacks in attacks in the *Network Device Level*, the *OS Level, application based attacks, data flooding attacks*, and *attacks based on protocol features. DoS attacks in the Network Device Level* include attacks that might be caused either by taking advantage of bugs or weaknesses in software, or by exhausting the hardware resources of network devices. One example of a network device exploit is the one that is caused by a buffer-overrun error in the password checking routine. Using this exploit, certain routers (Karig et al., 2001) could be crashed if the connection to the router is performed via telnet and entering extremely long passwords. *The OS level DoS attacks* (Karig et al., 2001) take advantage of the ways protocols are implemented by operating systems. One example of this category of DoS attacks is the Ping of Death attack (Insecure.org, 1997). In this attack, ICMP echo requests having data sizes greater than the maximum IP standard size are sent to the victim. This attack often results in the crashing the victim's machine. *Application-based attacks* try to take a machine or a service

out of order either by exploiting bugs in network applications that are running on the target host or by using such applications to drain the resources of their victim. It is also possible that the attacker may have found points of high algorithmic complexity and exploits them in order to consume all available resources on a remote host. One example of an application-based attack (Karig et al., 2001) is the finger bomb. A malicious user could cause the finger routine to be recursively executed on the victim, in order to drain its resources. In *data flooding attacks*, an attacker attempts to use the bandwidth available to a network, host, or device at its greatest extent, by sending massive quantities of data and so causing it to process extremely large amounts of data. An example is flood pinging. DoS attacks *based on protocol features* take advantage of certain standard protocol features. For example, several attacks exploit the fact that IP source addresses can be spoofed. Moreover, several types of DoS attacks attempt to attack DNS cache on name servers. A simple example of attacks exploiting DNS is when an attacker owning a name server traps a victim name server into caching false records by querying the victim about the attacker's own site. If the victim name server is vulnerable, it would then refer to the malicious server and cache the answer.

3.3 DISTRIBUTED DENIAL OF SERVICE ATTACKS

Defining Distributed

Denial of Service Attacks

The WWW Security FAQ (Stein & Stewart, 2002) states "A DDoS attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the DoS significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms." It is distinguished from other attacks by its ability to deploy its weapons in a "distributed" way over the Internet and to aggregate these forces to create lethal traffic. The main goal of a DDoS attack is to cause damage on a victim either for personal reasons or for material gain or for popularity. Mirkovic, Martin, and Reiher (2001) state that the following Internet characteristics make DDoS attacks very destructive:

1. **Interdependency of Internet security:**
When a machine is connected to the Internet, it is also connected to countless insecure and vulnerable hosts, making it difficult to provide a sufficient level of security.

2. **Limited resources:** Every host in the Internet has unlimited resources, so sooner or later its resources will be consumed.

3. **Many against a few:** If the attacker's resources are greater than the victim's resources then a DDoS attack is almost inevitable.

DDoS Strategy

A distributed denial of service attack is composed of four elements, as shown in Figure 1.

1. The *real attacker*
2. The *handlers or masters,* who are compromised hosts with a special program capable of controlling multiple agents, running on them (Cisco Systems, Inc., 2006)

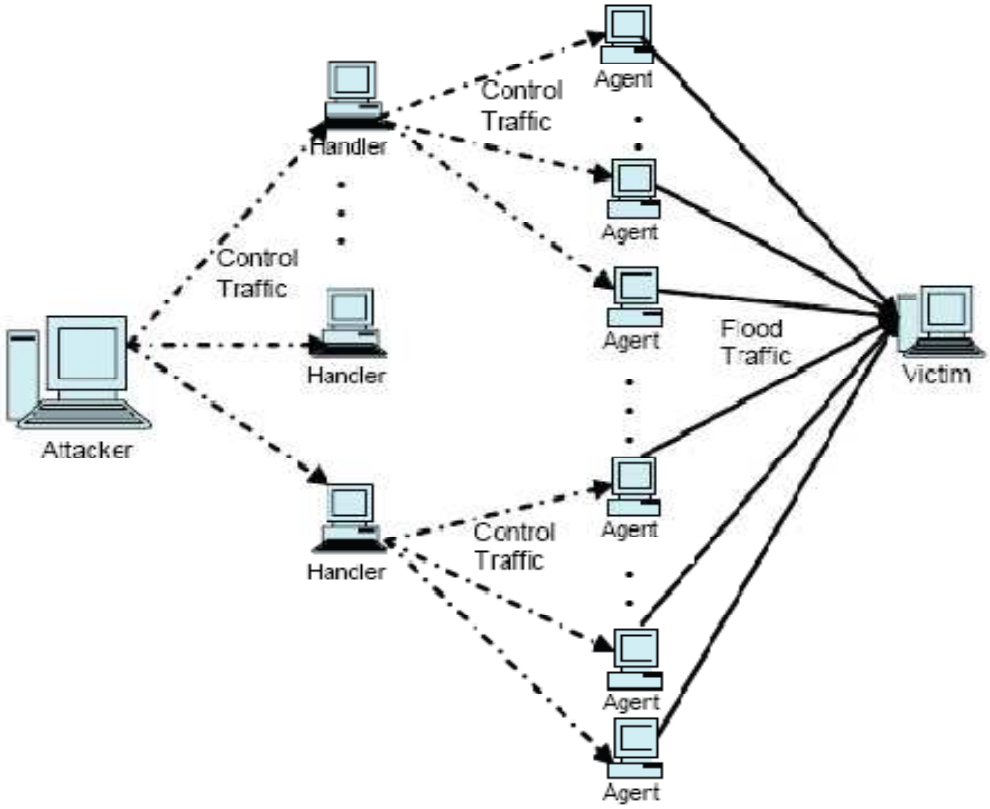
3. The attack daemon agents or zombie hosts, who are compromised hosts, running a special program and generate a stream of packets towards the victim (Cisco Systems, Inc., 2006)

4. A *victim* or *target host* The following steps take place in order to prepare and conduct a DDoS attack:

• **Step 1. Selection of agents:** The attacker chooses the agents that will perform the attack. The selection of the agents is based on the existence of vulnerabilities in those machines that can be exploited by the attacker in order to gain access to them.

• **Step 2. Compromise:** The attacker exploits the security holes and vulnerabilities of the agent machines and plants the attack code.

Figure 1. Architecture of DDoS attacks



Furthermore, the attacker tries to protect the code from discovery and deactivation. Self propagating tools such as the Ramen worm (CIAC Information Bulletin, 2001) and Code Red (CERT, 2001) soon automated this phase. When participating in a DDoS attack, each agent program uses only a small amount of resources (both in memory and bandwidth), so that the users of computers experience minimal change in performance The people who use the agent systems do not know that their systems are compromised and used for the launch of a DDoS attack (Specht & Lee, 2003). When participating in a DDoS attack, agent programs consume little resources this means that the users of computers experience minimal change in performance.

• **Step 3. Communication** (Specht et al., 2003)**:** Before the attacker commands the onset of the attack, he communicates with the handlers in order to find out which agents can be used in the attack, if it is necessary to upgrade the agents and when is the best time to schedule the attack.

• **Step 4. Attack:** At this step, the attacker commands the onset of the attack (Mirkovic, 2002). The victim and the duration of the attack as well as special features of the attack such as the type, port numbers, length, TTL, and so forth can be adjusted. In a new generation of DDoS attacks, the onset of the attack is not commanded by the attacker but starts automatically during a monitoring

procedure of a public location on the Internet. For instance, a chat room may be monitored and when a specific word is typed the DDoS attack is triggered. It is even more difficult to trace the attacker and reveal its true origin in such an environment. We can understand the enormity of the danger if the trigger word or phrase is commonly used. Specht et al. (2003) state that a multi-user, online chatting system known as Internetrelay chat (IRC) channels is often used for the communication between the attacker and the agents, since IRC chat networks allow their users to create public, private and secret channels. An IRC-based DDoS attack model does not have many differences computed to the agent-handler DDoS attack model except from the fact that an IRC server is responsible for tracking the addresses of agents and handlers and for facilitating the communication between them. The main advantage of the IRC-based attack model over the agent-handler attack model is the anonymity it offers to the participant of the attack.

Self Assessment Exercise

Define and explain the concept of Denial of Service Attacks as a security issue

4.0 CONCLUSION

Undoubtedly, DoS attacks should be treated as a serious problem in the Internet. Their rate of growth and wide acceptance challenge the general public's view of electronic transactions and create sceptical governments and businesses. No one can deny that DoS attacks will continue to pose a significant threat to all organisations including government organisations. New defence mechanisms will be followed by the emergence of new DoS attack modes. A network infrastructure must be both robust enough to survive direct DoS attacks and extensible enough to adopt and embrace new defences against emerging and unanticipated attack modes. In order to ensure high resiliency and high performance in public and private networks efforts need to be concerted by administrators, service providers and equipment manufacturers. It is of great importance that citizens communicate with their government authorities online. No one should be allowed to shut down valuable e-government services. A more enlightened approach would be to ask all citizens to take responsibility for securing the Internet in their hands. Public awareness is the key in order to securely exist and succeed in the world of e-government.

5.0 Summary

The use of electronic technologies in government services has played a significant role in making citizens' lives more convenient. Even though the transition to digital governance has great advantages for the quality of government services it may be accompanied with many security threats. One of the major threats and hardest security problems e-government faces are the denial of service (DoS) attacks. DoS attacks have already taken some of the most popular e-government sites off-line for several hours causing enormous losses and repair costs. In this chapter, important incidents of DoS attacks and

results from surveys that indicate the seriousness of the problem are presented. In order to limit the problem of DoS attacks in government organizations, we also present a list of best practices that can be used to combat the problem together with a classification of attacks and defence mechanisms.

6.0 Tutor Marked Assignment

List and explain with the aid of a diagram the elements involved in the denial of service attack.

7.0 References/ Further Reading

Barlow, J., & Thrower, W. (2000). *TFN2K—An analysis.* Retrieved from http://seclists.org/lists/ bugtraq/2000/Feb/0190.html

Bysin. (2001). *Knight.c Sourcecode.* Retrieved from http://packetstormsecurity.nl/ distributed/ knight.

CERT. (2001). *CERT Coordination Center Advisory CA-2001-19 Code Red Worm Exploiting Buffer Overflow in IIS Indexing Service DLL.* Carnegie Mellon Software Engineering Institute. Retrieved from http://www.cert.org/advisories/ CA-2001-19.html

CIAC Information Bulletin. (2001). L-040: The Ramen Worm. *Computer Incident Advisory Capability (CIAC).* Retrieved from http://www.ciac. org/ciac/bulletins/l-040.shtml

Cisco Systems, Inc. (2006). *Strategies to protect against distributed denial of service (DDoS) attacks* (Document ID: 13634). Retrieved from http://www.cisco.com/warp/public/707/newsflash. Html Computer Security Institute. (2003). *2003 CSI/FBI Computer Crime and Security Survey*. CSI Inc.

Computer Security Institute. (2004). *2004 CSI/FBI Computer Crime and Security Survey.* CSI Inc.

Criscuolo, P. J. (2000). *Distributed denial of service Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht CIAC-2319* (Tech. Rep. No. , UCRL-ID-136939, Rev. 1.). Department of Energy Computer Incident Advisory Capability (CIAC), Lawrence Livermore National Laboratory. Retrieved from http://ftp.se.kde.org/ pub/security/csir/ciac/ ciacdocs/ciac2319.txt

Cs3 Inc. (2005). *Defending government network infrastructure against distributed denial of service attacks.* CS3-inc.com. Retrieved from http:// www.cs3-inc.com/government-ddos-threat-andsolutions. pdf

Dietrich, S., Long, N., & Dittrich, D. (2000). Analyzing distributed denial of service tools: The shaft case. In *Proceedings of the 14th Systems Administration Conference (LISA 2000)* (pp. 329-339), New Orleans, LA.

Dittrich, D. (1999a). *The tribe flood network distributed denial of service attack tool. University of Washington.* Retrieved from http://staff.washington. edu/dittrich/misc/ trinoo.analysis.txt

Dittrich, D. (1999b). *The Stacheldraht distributed denial of service attack tool. University of Washington.* Retrieved from http://staff.washington.edu/dittrich/misc/ stacheldraht.analysis.txt

Unit 15
DDoS Tools: A Security Threat

1.0 Introduction

E-government undoubtedly makes citizens' lives and communication easier by saving time, by avoiding and bypassing the bureaucracy, and by cutting down paper work. It also provides the same opportunities for communication with government not only to people in cities but also to people in rural areas. Moreover, e-government permits greater access to information, improves public services, and promotes democratic processes. Notwithstanding there are several known DDoS attack tools capable of frustrating the effort of these technologies. The architecture of these tools is very similar whereas some tools have been constructed through minor modifications of other tools. In this section, we present the functionality of some of these tools. For presentation purposes, we divide them in *agent-based* and *IRC-based* DDoS tools. Agent-based DDoS tools are based on the agent—handler DDoS attack model that consists of handlers, agents, and victim(s) as it has already been described in the section on DDoS attacks. Some of the most known agent-based DDoS tools are the following: *Trinoo, TFN, TFN2K, Stacheldraht, mstream, and Shaft*. *Trinoo* (Criscuolo, 2000) is the most known and mostly used DDoS attack tool.

2.0 Objectives

This unit throws more light to some specific tools capable and being used in launching attacks on internet bandwidth. Readers of this manual are therefore expected note the classification and categories of DDoS defence mechanisms and how they can be best deployed.

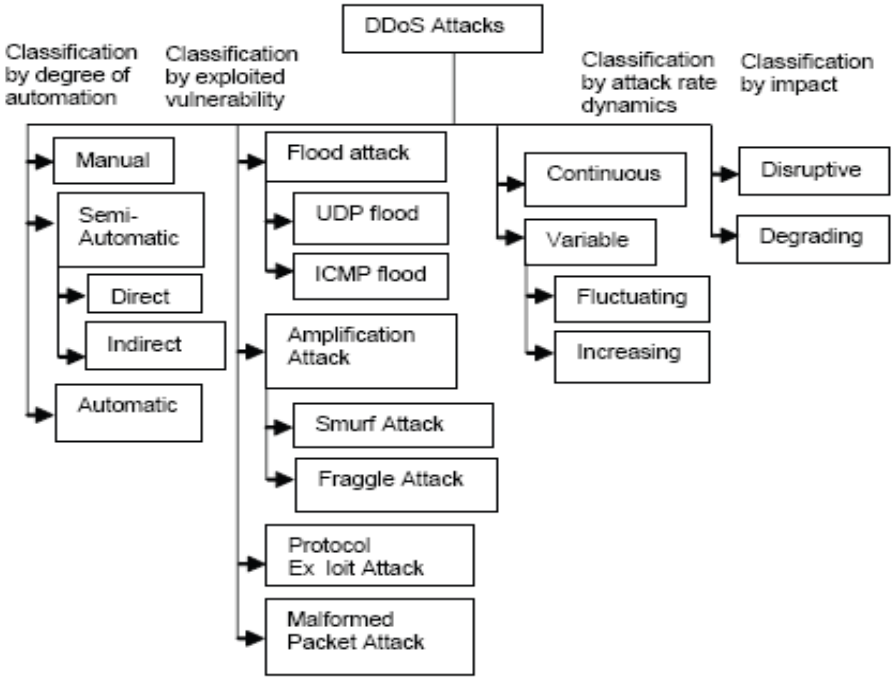
3.0 Main body

It is a tool that is able to achieve bandwidth depletion and can be used to launch UDP flood attacks. *Tribe Flood Network (TFN)* (Dittrich, 1999a) is a DDoS attack tool that is able to perform resource and bandwidth depletion attacks. Some of the attacks that can be launched by TFN include Smurf, UDP flood, TCP SYN flood, ICMP echo request flood, and ICMP directed broadcast. *TFN2K* (Barlow & Thrower, 2000) is a derivative of the TFN tool and is able

to implement Smurf, SYN, UDP, and ICMP Flood attacks. TFN2K has a special feature of being able to add encrypted messaging between all of the attack components (Specht et al., 2003). *Stacheldraht* (Dittrich, 1999b) (German term for "barbed wire"), that is based on early versions of TFN, attempts to eliminate some of its weak points and implement Smurf, SYN Flood, UDP Flood, and ICMP Flood attacks. *Mstream* (Dittrich, Weaver, Dietrich, & Long, 2000) is a simple TCP ACK flooding tool that is able to overwhelm the tables used by fast routing routines in some switches. *Shaft* (Dietrich et al., 2000) is a DDoS tool similar to Trinoo that is able to launch packet flooding attacks by controlling the duration of the attack as well as the size of the flooding packets. Many IRC-based DDoS tools are very sophisticated as they include some important features that are also found in many agent-handler attack tools. One of the most known IRC-based DDoS tools is *Trinity* (Hancock, 2000). *Trinity v3* (Dietrich et al., 2000) besides the up to now well-known UDP, TCP SYN, TCP ACK, TCP NUL packet floods introduces TCP fragment floods, TCP RST packet floods, TCP random flag packet floods, and TCP established floods. In the same generation with Trinity is *myServer* (Dietrich et al., 2000) and *Plague* (Dietrich et al., 2000). MyServer relies on external programs to provide DoS and Plague provides TCP ACK and TCP SYN flooding. *Knight* (Bysin, 2001) is a very lightweight and powerful IRC-based DDoS attack tool able to perform UDP Flood attacks, SYN attacks and an urgent pointer flooder. A DDoS tool that is based on Knight is *Kaiten* (Specht et al., 2003). Kaiten includes UDP, TCP flood attacks, SYN, and PUSH+ACH attacks and it also randomizes the 32 bits of its source address.

To be able to understand DDoS attacks it is necessary to have a formal classification. We propose a classification of DDoS attacks that combines efficiently the classifications proposed by Mirkovic et al. (2001), Specht et al. (2003), and more recent research results. This classification is illustrated in Figure 2 and consists of two levels. In the first level, attacks are classified according to their degree of automation, exploited vulnerability, attack rate dynamics and their impact. In the second level, specific characteristics of each first level category are recognized

Figure 2. Classification of DDoS attacks



3.1 CLASSIFICATION OF DDOS DEFENCE MECHANISMS

DDoS attack detection is extremely difficult. The distributed nature of DDoS attacks makes them extremely difficult to combat or trace back. Moreover, the automated tools that make the deployment of a DDoS attack possible can be easily downloaded. Attackers may also use IP spoofing in order to hide their true identity. This spoofing makes the traceback of DDoS attacks even more difficult. We may classify DDoS defence mechanisms using two different criteria. The first classification categorizes the DDoS defence mechanisms according to the activity deployed as follows:

1. **Intrusion prevention:** Tries to stop DDoS attacks from being launched in the first place.
2. **Intrusion detection:** Focuses on guarding host computers or networks against being a source of network attack as well as being a victim of DDoS attacks either by recognizing abnormal behaviours or by using a database of known.
3. **Intrusion response:** Tries to identify the attack source and block its traffic accordingly.
4. **Intrusion tolerance and mitigation:** Accepts that it is impossible to prevent or stop DDoS attacks completely and focuses on minimizing the attack impact and on maximizing the quality of the offered services. The second classification divides the DDoS defences according to the location deployment resulting (Mirkovic, 2002) into the following three categories of defence mechanisms:

1. **Victim network mechanisms:** Helps the victim recognize when it is the main target of an attack and gain more time to respond.

2. **Intermediate network mechanisms:** Are more effective than victim network mechanisms since they achieve a better handling of the attack traffic and an easier tracing back to the attackers.

3. **Source network mechanisms*:*** Trys to stop attack flows before they enter the Internet core and facilitate the trace back and investigation of an attack. The previous classification of DDoS defence mechanisms is described thoroughly in Douligeris and Mitrokotsa (2004).

3.2 BEST PRACTICES FOR DEFEATING DENIAL OF SERVICE ATTACKS

DoS attacks can lead to a complete standstill of entire government organisations, thereby costing millions of dollars in lost revenue and/or productivity and moving citizens away from e-services. Some governments do not understand the seriousness of the problem, resulting in vulnerable and easy to compromise systems. These systems pose a threat not only to the organisations themselves but also to anyone else targeted by a hacker through these systems. This means it is critical to take preemptive measures to reduce the possibility of these attacks and minimize their impact. Since DoS attacks are extremely complicated one must note that there is no single-point solution and no system is secure proof. No one can deny though that with effective advance planning government agencies could respond efficiently and rapidly to security threats like denial of service. Below we list some practices that can be used in order to reduce these attacks and diminish their impact.

1. **Establish a security policy and educate:** As stated by Walters (2001), it is of great importance to establish and maintain a security policy. In addition to covering the basics of antivirus, user access, and software updates, on no account one should neglect to address ways to combat DoS/DDoS attacks in such a policy. Moreover, a security policy should be adequately communicated to all employees. It is important to verify that the knowledge skills of system administrators and auditors are current, something that can be achieved by frequent certifications. Of great importance is the continuous training of the organisation’s personnel in new technologies and forensic techniques.

2. **Use multiple ISPs:** Government organisations should consider using more than one ISP, in order to make a DoS/DDoS attack against them harder to carry out. In the selection of ISPs, it is important to keep in mind that providers should use different access routes in order to avoid a complete loss of access in the case one pipe becomes disabled (Walters, 2001). It has also been proposed to set legislation to make it obligatory for ISPs to set up egress filtering.

3. **Load balancing:** Specht et al. (2003) state that a good approach in order to avoid being a victim of DoS attacks is to distribute an organisation's systems' load across multiple servers. In order to achieve this, a "Round Robin DNS" or hardware routers could be used to send incoming requests to one or many servers.

4. **Avoid a single point failure:** In order to avoid a single point failure the best solution is to have redundant ("hot spares") machine that can be used in case a similar machine is disabled (Householder, Manion, Pesante, Weaver, & Thomas, 2001). Furthermore, organisations should develop recovery plans that will cover each potential failure point of their system. In addition, organisations should use multiple operating systems in order to create "biodiversity" and avoid DoS attack tools that target specific Operating Systems (OSs).

5. **Protect the systems with a firewall:** Walters (2001) states that since the exposure to potential intruders is increasing, the installation of firewalls that tightly limit transactions across the systems' periphery government organisations should be built to provide effective defences. Firewalls should be configured appropriately keeping open only the necessary ports. In addition, firewalls are able to carefully control, identify, and handle overrun attempts. Moreover, ingress filtering should be established in government Web servers so that they cannot be used as zombies for launching attacks on other servers. Government departments should also specify a set of IP addresses that could be used only by Government servers.

6. **Disable unused services:** It is important, that as Leng and Whinston (2000) state, organisations' systems remain simple by minimizing the number of services running on them. This can be achieved by shutting down all services that are not required. It is important to turn off or restrict specific services that might otherwise be compromised or subverted in order to launch DoS attacks. For instance, if UDP echo or character generator services are not required, disabling them will help to defend against attacks that exploit these services.

7. **Be up to date on security issues:** As it iswidely known the best way to combat DoS attacks is to try to be always protected and up-to-date on security issues (Householder et al., 2001). It is important to be informed about the current upgrades, updates, security bulletins, and vendor advisories in order to prevent DoS attacks. Thus, the exposure to DoS attacks can be substantially reduced, although one would not expect the risk to be eliminated entirely.

8. **Test and monitor systems carefully:** The first step in order to detect anomalous behaviour is to "characterize" what normal means in the context of a government agency's network. The next step should be the auditing of access privileges, activities, and applications. Administrators should perform 24x7 monitoring in order to reduce the exhausting results of DoS attacks that inflict government servers. Through this procedure, organisations would be able to

detect unusual levels of network traffic or CPU usage (Householder et al., 2001). There are a variety of tools that are able to detect, eliminate, and analyze denial-of-service attacks.

9. **Mitigate spoofing:** An approach that intruders often use in order to conceal their identity when launching DoS attacks is source-address spoofing. Although it is impossible to completely eliminate IP spoofing, it is important to mitigate it (Singer, 2000). There are some approaches that can be used in order to make the origins of attacks harder to hide and to shorten the time to trace an attack back to its origins. System administrators can effectively reduce the risk of IP spoofing by using ingress and egress packet filtering on firewalls and/or routers.

10. **Stop broadcast amplification:** It is important to disable inbound directed broadcasts in order to prevent a network from being used as an amplifier for attacks like ICMP Flood and Smurf (Leng et al., 2000). Turning off the configuration of IP directed broadcast packets in routers and making this a default configuration is the best action that could be performed by network hardware vendors.

11. **DNS for access control should not be used:**
Using hostnames in access list instead of IP addresses make systems vulnerable to name spoofing (Leng et al., 2000). Systems should not rely on domain or host names in order to determine if an access is authorized or not. Otherwise, intruders can masquerade a system, by simply modifying the reverse lookup tables.

12. **Create an incident response plan:** It is important to be prepared and ready for any possible attack scenario. Government organisations should define a set of clear procedures that could be followed in emergency situations and train personnel teams with clearly defined responsibilities ready to respond in emergency cases (Householder et al., 2001). Any attacks or suspicious system flaws should be reported to local law enforcement and proper authorities (such as FBI and CERT) so that the information could be used for the defence of other users as well.

3.3 LONG-TERM COUNTERMEASURES

The variety and sophistication of DoS attacks are likely to increase, so despite the defensive measures that can be used now, we need to confront DoS attacks as a problem that requires a long-term effort in order to define and implement effective solutions. It is important to note here that governments should adopt a non-intrusive approach for the protection against DoS attacks while there is a fine line between limiting criminal activity and limiting economy, education, information, and personal freedoms. Suns Institute (2000) identifies some actions that will help in defending against DoS attacks more effectively in the distant future. Among them one finds the accelerated adoption of the IPsec

components of IPv6 and Secure DNS. It is important that the security updating process be automated. Vendors should be encouraged to implement this on behalf of their clients in order to make it easier to update their products and provide information on security issues. Furthermore, research and development of safer operating systems is necessary. Topics to be addressed should include among others anomaly-based detection and other forms of intrusion detection.

In addition, governments should consider making some changes in their government procurement policies in a way that security and safety are emphasized. A significant role in the fight against denial of service attacks would be the establishment of organisations that would be responsible for network security monitoring and incident handling. These organisations should encourage the public awareness about security issues, inform critical owners' infrastructures and government departments about threats, promote and encourage the adoption and production of security standards and maintain statistics and incident databases as well as cooperate with similar organisations (e.g., CERT). Governments should also ensure that government agencies take all the necessary steps in order to ensure their IT security. Government departments should encourage a better investigation of computer attacks while respecting the privacy and personal rights of Internet users. Additional funding for the training of expert personnel in securing IT Technologies and educating citizens in order to be prevented from cyber crime is a must. It is also important to promote and encourage law enforcement authorities to prosecute perpetrators across national borders and examine the legal framework to facilitate this cooperation.

Self Assessment Exercise

What are the best practices for defeating denial of service attacks?

4.0 Conclusion

DoS attacks constitute a serious threat in the face of wide usage of internet facilities. No one can deny that DoS attacks will continue to pose a significant threat to all organisations including government organisations. It becomes imperative that students administrators and government officials become prepare in fighting the menace or curbing it.

5.0 Summary

A clear cut understanding of the impact of DoS on electronic governance was introduced in the previous section highlighting the import of Technological advancement on decision making, with great impact on governnace administration, nevertheless this unit explain some of the hindrances and problems embedded in the DoS system of information control. In order to limit the problem of DoS attacks in government organizations, we also present a list of best practices that can be used to combat the problem together with a classification of attacks and defence mechanisms.

6.0 Tutor Marked Assignment

DDoS attack detection is extremely difficult. Explain

Succinctly discuss some of the best some practices that can be used to reduce these attacks and diminish their impact.

7.0 References/ Further Reading

Dittrich, D., Weaver, G., Dietrich, S., & Long, N. (2000). *The mstream distributed denial of service attack tool.* University of Washington. Retrieved from http://staff.washington.edu/dittrich/ misc/mstream.analysis.txt

Douligeris C., & Mitrokotsa, A. (2004). DDoS attacks and defence mechanisms: Classification and state-of-the-art. *Computer Networks, 44*(5), 643-666.

Fox News. (2002). *Powerful attack cripples Internet*. Retrieved from http://www.linux.security. com/content/view/112716/65/

Hancock, B. (2000). Trinity v3, A DDoS tool, hits the streets. *Computers & Security, 19*(7), 574-574.

Holden, S., Norris, D., & Fletcher, P. (2003). Electronic government at the local level: Progress to date and future issues. *Public Performance and Management Review, 26*(4), 325-344.

Householder, A., Manion, A., Pesante, L., Weaver, G. M., & Thomas, R. (2001). *Trends in denial of service attack technology* (v10.0). CERT CoordinationCenter, Carnegie Mellon University. Retrieved from http://www.cert.org/archive/pdf/DoS_trends.pdf

Howard, J. (1998). *An analysis of security incidents on the Internet 1989-1995.* PhD thesis, Carnegie Mellon University. Retrieved from http://www.cert.org/research/ JHThesis/Start.html

Insecure.org. (1997). *Ping of death.* Retrieved from http://www.insecure.org/sploits/ ping-odeath.html

Institute for e-government Competence Center (IfG.CC). (2002). *eGovernment: "First fight the hackers."* Retrieved from http://www.unipotsdam. de/db/elogo/ifgcc/index.php?option=com_content&task=view&id=1450&Itemid=93&lan g=en_GB

ITworld.com. (2001). *CERT hit by DDoS attack for a third day.* Retrieved from http://www.itworld. com/Sec/3834/IDG010524CERT2/

UNIT 16
Securing the Computer Systems

1.0 Introduction

There has been a growing interest in "self help" mechanisms to counter Internet-mediated threats. Content providers such as record labels and movie studios have favoured proposed federal legislation that would allow them to disable copyright infringers' computers. Software licensors have backed multiple-state legislation, permitting the remote disabling of software in use by the licensee when the license terms are breached. Internet security professionals debate the propriety, and legality, of striking back at computers which attack the Internet through the introduction of worms, viruses, and so on, collectively "malware. Systems administrators are frustrated that the usual means of enforcing rights do not work on the Internet. Although national laws and civil jurisdiction usually stop at the border, attacks are global, and those responsible for infringements and network attacks are not only legion, but anonymous. The Internet's massive, instantaneous distribution of software tools and data permits very large numbers of unsophisticated users access to highly efficient decryption tools, as well as to very powerful data attack weapons.

2.0 Objectives

This unit aims at explaining the general application of counterstrike, Counterstrike and Self-Defense Law, and Counterstrike and Nuisance Law as Security Management Options in an internet world.

3.0 Main body

It is no long news that Small children in countries like Hanoi, Prague and Fairbanks can collapse central web servers in Silicon Valley and Alexandria, Virginia, and freely distribute the latest films and pop tunes. The irony is that as more of the global economy is mediated by the Internet – that is, as we increasingly rely on the Internet – the technologies become more complex, and more vulnerable to attack from more people. Even a cursory look at the figures suggests an almost exponential increase in these vulnerabilities. Simultaneously, the legal system is increasingly incapable of policing the illegal behaviour. The court system is ponderous and expensive. One simply cannot go after every malefactor, and as a practical matter, it is usually impossible to pursue infringers outside ones country. The Internet and its language of code are global. They are not coterminous with any of the usual means of enforcement of laws and values, because the Internet is not coterminous with any country, region, or cultural group. The Internet gathers those who have no contractual relationship, speak no common language, and are not bound by a common law. Trade sanctions will not assist. Nations will not permit their citizens to be policed directly by authorities across the globe. In my own work, I have tracked anonymous malefactors to towns in Australia, Eastern Europe and the Bahamas; and there, the trail went cold. Only in Australia could we have retained local counsel and perhaps pressed matters with the police, but it was too expensive, all told.

Resorting to domestic police is frustrating. The FBI has understandably re-routed resources to combating terrorism, and local authorities do not have the wherewithal to rapidly react to assaults from other parts of the country. By many accounts, conventional law enforcement authorities simply do not have the skills to deal with cyberattacks, and victims such as banks, financial institutions, and others that deal in sensitive data are reluctant to go public and in effect turn over the investigation to the authorities. Fundamentally, going to law enforcement does not stop an attack, at least in the short term. Rather, it starts an investigation that could take months or longer to result in an arrest. That's an eternity in Internet time. As legal systems become less effective in addressing these concerns, attention naturally turns to technology, and traditionally, defensive technology. There is a broad range of products that help to protect networks, to keep content encrypted, and so on. In the networks security area, firewalls, intrusion detection systems, authentication devices, and perimeter protection devices are among the services and products available. But two general trends of increasing complexity undermine the efficacy of defensive technologies: increasingly complex systems and increasing connectivity. The complex relationship among multiple layers of hardware and software means that new bugs and avenues to exploitation are being discovered

on a daily basis. Larger systems usually include dispersed, networked, computers operated by outsourcers, server farms and hosts, other application service providers, as well as the machines used by the ultimate users.

Increased connectivity is manifest in both the onslaught of “always on” DSL, cable and other high-speed Internet clients, and in the design of the most popular software (Microsoft), which favours interoperability and easy data sharing over compartmentalized (more secure) applications. This massive connectivity of machines, many of which are not maintained by users who know anything about security, permits, for example, the well known distributed denial of service (DDoS) attack, in which up to millions of computers (‘zombies’) can be infected with a worm which then launches its copies simultaneously against the true target – e.g., Amazon, or eBay – shutting the target down. Together, these factors make it difficult to implement defensive technologies. Relatively few companies have the resources and interest to review and implement every bug fix, and otherwise to keep ahead of the endlessly inventive cracker. “Information technology infrastructures are becoming so complex that no one person can understand them, let alone administer them in a way that is operationally secure.” “The complexity of modern [operating systems] is so extreme that it precludes any possibility of not having vulnerabilities.”

These vulnerabilities of course give rise to legal liabilities for the victim. Loss of service and corrupted data can underpin users’ claims for breach of contract, privacy incursions, copyright violation, negligence and so on. A sustained attack can put a victim out of business. And owners and operators of zombied machines, too, can be sued if the attack can be traced to negligence in the security systems implemented (or rather, not implemented) on the zombies. To rub salt on those wounds, California recently enacted a law, now being considered for nationwide implementation, which would require notification by a systems operator to persons whose personal data may have been accessed during a security breach. Some have termed this an “invitation to sue” provision.

II. THE GENERAL APPLICATION OF COUNTERSTRIKE

Against this background, self help or “strike back” or “counterstrike” tools have garnered great interest, and sharp words have been exchanged on proposals to implement automated counterstrike. Under that plan, a network that finds itself under attack automatically traces back the source and shuts down, or partially disables, the attacking machine(s). Reminiscent of the Cold War “launch on warning” nuclear deterrent, the premise is that only a computer can react fast enough to detect the attack, trace it to a source, and disable the attacking machine, all in time to have any chance at all of minimizing the effects of the attack. Something like this has been implemented in the past. In response to the Code Red II (CRII) worm attack, someone created an anti-code-red-II-default.ida.script which reputedly responded to a CRII probe by disabling the offending web server, using a backdoor installed by the CRII

worm in the victim's machine. Stories abound of other aggressive responses to cyberattacks.

There are practical issues to consider here. Not all attacks will so plainly reveal a path back to their source as did CRII; tracing an attack to an intermediate attacking machine, not to speak of the computer owned by the originator in a DDoS attack, may be impossible. Further, intermediate machines, or zombies in a DDoS attack, may be operated by hospitals, governmental units, and telecommunications entities such as Internet service providers that provide connectivity to millions of people. Therefore, counterstrikes which are not very precisely targeted to the worm or virus could easily create a remedy worse than the disease. Where the offense is spam and its content is libellous, malicious or pornographic, the trace will generally lead to an anonymous account on a server – a server which is legitimately used for other communications as well. Disabling that server is overkill. But practicalities aside, what are the legal risks? Perhaps we can assume that we will devise precise counterstrike weapons; perhaps the recording industry can precisely identify its copyrighted songs, calculate which are licensed to which users (or machines), and destroy solely the offending copy. Perhaps data streams can be tagged with the identification number of the originating machine in every case, such that viruses, worms, and other offending code can be accurately tracked back to the source, and disabling mechanisms will target solely the malware.
While it is generally thought to be illegal to strike back, the rationale is usually based on the practicality of pinpointing the perpetrator, and killing the wrong machine or code. But even the accurate targeting of a perpetrator's machine itself presents serious legal issues. Indeed, a host of statutes on their face make it illegal to attack or disable computers, including those connected to the Internet. These are the very laws which make cyberattacks illegal in the first place.

The legalities of attacks and counterstrikes matter not only in the civilian world. Information warfare conducted, and defended against, by governments must also heed the civilian legalities. This is because it is not possible to clearly distinguish classic war between nations from the prevalent lower intensity clashes and retaliation, and this gray area is far more pronounced and extensive in information warfare, which takes place without overt hostilities and without physical weapons. It is increasingly useless in this context to speak of an "act of war", as opposed to "hostile acts" and other terms which denote continuous low intensity assaults and reconnaissance on the nation's electronic infrastructure. Such hostile acts are on-going, sponsored by individuals, groups, and governments from friendly to the most unfriendly nations. In this gray area, the legality of strike and counterstrike against an entity that is not literally "at war" with the United States cannot be determined by, for example, the commonly accepted law of armed conflict. Indeed, that law, based primarily on the Hague and Geneva conventions, does not contemplate information warfare. Rather, the legality of strike and counterstrike in the typical low intensity

information warfare scenario is likely to devolve to the legality of the action under the criminal law.

III. COUNTERSTRIKE AND SELF-DEFENSE LAW

And so the analogy to the legal doctrine of self-defense comes into play: does self-defense apply to the Internet, and does it justify counterstrike? Self defense usually is at stake when a person is threatened with imminent bodily harm. The test is whether (1) there is an apparent necessity to use force, (2) the force used was in fact reasonable, and (3) the threatened act was unlawful. There are other factors, but the underlying themes in self-defense are (1) a counterstrike which is proportional to the harm avoided, and (2) both a good faith subjective, and objectively reasonable, belief that the counterstrike was necessary in the sense that there were no adequate alternatives. Disabling an evil-doer's machine is, I suggest, far less injurious than a DDoS assault, and I suggest that disabling the attacker's machine (although not necessarily destroying his data) is a response that is proportional to the threatened corruption of a victim's file. A "self defense" theory could thus justify a counterstrike when the threat is malware, as the erasure of a pirated copy of a film, song or computer game is proportional to the harm posed by the use of the infringing copy by the pirate (not to mention the additional harm posed by the risk that the pirated copy may be further distributed). The more difficult issue is that of adequate alternatives. The elementary alternatives, of course, are for the victim to use effective perimeter defenses and other protections, thus diminishing the probability that an attack will succeed, and failing that, to disconnect from the Internet to avoid the attack. But that last option is itself often the harm directly sought to be caused by the malware attack – and classically, self defense doctrine does not require the victim to back away. Rather, in most states, one may "stand his ground" and not retreat, and still be entitled to self defend if the attack progresses. So, what should one think about "adequate alternatives" such as perimeter defenses? Is one always required to rely on these defensive alternatives and to forgo the offensive ones? The central problems in addressing this question are twofold.

First, we cannot generalize over a wide range of incidents. Second, the "subjective" perspective of the information technology professional may differ greatly from that of an "objective" prosecutor, judge, or jury. There is a wide range of security incidents, ranging from inadvertent innocuous incursions by badly written computer scripts to intentional attempts to flood a system with communication requests and shut it down, to deliberate penetrations to obtain (or corrupt) highly sensitive data. The unauthorized entry might be accomplished because the most elementary security precaution was not taken, or on the other end of the spectrum, because the perpetrator has devised a brilliant and entirely unexpected method to exploit a hitherto unknown problem in an operating system or browser. A judge or jury might find that "adequate alternatives" existed to head off a simple, predictable attack, but not for a sophisticated, unanticipated one. This is a difficult problem, because standards

in this area are difficult to come by, and the actual competence of systems administrators, together with the funding provided to them by upper management, is often low. A good example is the February 03 Sapphire worm attack, in which systems administrators, who had presumably been put on notice by prior CRII and Nimda attacks, failed to implement simple patches which would have blocked the spread of the similar Sapphire attack. It may be the case, as suggested above, that systems are simply too complex and mutate too quickly to guard against every point of failure, but in hindsight, at least, any given failure will often appear to have been easily preventable. And there is another consideration. If the counterstrike tool is good enough to identify the attack and pinpoint the cracker's machine, how could it not be good enough to block the attack?

In brief, it can be a dicey thing to establish both a good faith and objectively reasonable belief that there were no adequate alternatives to a counterstrike. The plethora of defensive products and services, good practice guidelines (even if observed more faithfully "in the breach," as it were), and reliable / hindsight conspire to make self defense a tricky maneuver to justify. To be sure, it is not impossible to do so, and expert testimony might help, but because the consequences of guessing wrong are so onerous – e.g., conviction of a federal felony – the absence of directly relevant case authority should give should give one pause; a very long pause.

IV. COUNTERSTRIKE AND NUISANCE LAW

There is another legal doctrine, though, that might hold more promise, and it is the venerable doctrine of nuisance. In its amicus brief in Intel v. Hamidi, the Electronic Frontier Foundation (EFF) developed the concept that an alleged spammer's assault on Intel's internal email system should be thought of not as a trespass on Intel's property, but as a nuisance. Nuisances can be almost anything that interferes with one's enjoyment of one's property. Classic public nuisances include malodorous factories, diseased plants, fire hazards, and houses of ill repute. Public nuisances affect the community. Private nuisances are those that affect only a single person, or one's own property. Usually they are real property problems such as tree branches and fences which interfere with the use of real property. The remarkable aspect of nuisance law is that it expressly contemplates self help. A person affected by a private nuisance, or a person who is especially affected by a public nuisance, may use self help and "abate" (stop) the nuisance – and then sue the malefactor for the costs of the abatement. Abatement includes "removing . . . or . . . destroying the thing which constitutes the [nuisance]" as long as there is no "breach of the peace" or "unnecessary injury." For example, one can break down doors, smash locks, or tear down fences, if these acts are reasonably necessary to abate the nuisance (provided that the other elements discussed below are met).

"Breach of the peace" is an elastic notion, usually connoting actual or threatened violence or disturbance, such as bad language, public nudity, demonstrations peaceful and not, and so on. I read the abatement statutes in their traditional context, where one might enter on the property of another to turn off water, put out a fire, or remove smelly detritus. Foreswearing a "breach of the peace" requires, in essence, that such entry must be done without causing a noticeable fuss or threatening the use of force. Assuming that a precision counterstrike could be executed against a cyberattacker, the "no breach of the peace" condition on the self help remedy would be met. Therefore, a traditional nuisance doctrine would not preclude the use of a targeted counterattack. The lawfulness inquiry devolves, then, to whether a cyberattack really qualifies as a nuisance. Granted, it fits the open-ended statutory definition, but of course, much does. Nuisance "has meant all things to all men, and has been applied indiscriminately to everything from an alarming advertisement to a cockroach baked in a pie." But of the three evils originally discussed above – the infliction of malware, copyright infringement, and unlicensed use of software – only malware appears close to the notion of a nuisance. The other two boil down to the same harm, copyright infringement, which is essentially a theft of private property.

Moreover, unless nuisance is to swallow every harm, it's a stretch to call infringement even a private nuisance. Indeed, it is the cyberattacks of malware, not infringement, that the predominate counterstrike advocate has in mind. Fundamentally, a nuisance is, among other things, an unreasonable invasion of the victim's interests where there is no reasonable basis for the action, including those actions arising from a malicious desire to do harm for its own sake. A virus probably fits the bill. It is not, of course, clear how a court would apply the old doctrine of nuisance to the Internet. We do know that the even more venerable doctrine of trespass has been so applied. Can the same act of computer code or data intrusion be both a trespass and a nuisance? The Intel court obscured the issue. The legal debate comes down to a bizarre squabble over whether the electro-magnetic signals which constitute the intrusion are "tangible" and do "physical" damage to the property, like "particulate matter" such as dirt (in which case we have a trespass), or whether on the other hand, they are like the "intangible" encroachments of light, noise, and odors which interfere with the property – in which case we have a nuisance. The squabble is pointless because a computer-based attack is all of those things. Just as light can be described as either a wave or a particle, so too might a computer virus, winging its electro-magnetic path into a network, be described as either an intangible nuisance or a tangible trespass, as a series of cases have stated.

If legislatures sympathized with the plight of victims of spam, or malware, and with the frustration of using the legal process to address the injury, they could statutorily define selected acts as nuisances (as they have done with other acts and conditions), and avoid the suspense. In the meantime, at least Internet-mediated attacks such as viruses and worms fit comfortably within the

definition of a nuisance, and if so would authorize and justify counterstrikes as "self help." There is at least one last twist to this view of a cyberattack as a nuisance, permitting (at least legally) self help or counterstrike. The issue has to do with the efficacy of using the defense of self help – which is a privilege of state law – in an action brought under federal law. The issue is the extent to which state privileges and defenses will stave off, for example, a federal criminal prosecution under the Computer Fraud and Abuse Act for unauthorized access to computer files. Normally of course, federal law only applies to federal claims, and federal law trumps state law. But there are exceptions. Sometimes, even in federal question cases, state law supplies the "rule of decision," such as in a copyright case where a contract must be interpreted, or where the court must decide if peace officers are authorized to serve process. This is not a simple issue, because each pertinent federal statute would need to be reviewed to determine if it appeared to be conditioned on, or contemplated, some state-defined notion or privileged access to self help. But in the Computer Fraud and Abuse Act, for example (the most likely candidate for a federal prosecution of a counterstrike attack), it is not a stretch to suggest that the key notion of "unauthorized" access to a computer could be defined under state law – with "self- help" providing the "authorization."

Self Assessment Exercise

1. Discuss the frustration domestic police encounter in fighting internet attacks

4.0 Conclusion

Even under various circumstances, not every counterstrike – or "self help" effort – is automatically immune. It has to be reasonable, and proportional to the nuisance, issues discussed in connection with a similar requirement under self-defense. And as always, the light cast by ancient doctrine upon novel technologies will produce illumination and shadow both. Courts will "fudge" on the analysis and struggle for precedent, sometimes testing out the wrong one. Just as no one wants to roll out version 1 (new software), no one wants to be a test case in court.

5.0 Summary

This unit discusses the inevitability of internet threats in the world. the various aspects involved in combating the threats, and the challenges facing domestic policing of the menace. Also self help or "strike back" or "counterstrike" tools were explained as proposals to implement automated counterstrike against internet attack.. Under this plan, a network that finds itself under attack automatically traces back the source and shuts down a computer, or partially disables, the attacking machine(s).

6.0 Tutor Marked Assignment

1. Explain some of the problems and difficulties inherent in the detection of internet attacks/attackers.

2. How does self-defense come into play internet security?

7.0 References/ Further Reading

Association for Internet Data Analysis, at http://www.caida.org/outreach/papers/2003/sapphire/index.xml (last modified Sept. 11, 2003)

Bureau of National Affairs, Berman to Introduce Bill Aimed at Curbing Piracy over Internet Peer-To-Peer Networks, 64 PAT. TRADEMARK & COPYRIGHT J. 190 (2002).

Jay Lyman, When the Haked Becomes the Haker, Nov. 19, 2001, at http://www.newsfactor.com/perl/story/14874.html/ (on file with the Yale Journal of Law & Technology).

Maj. David DiCenso, The Legal Issues of Information Warfare, 13 AIRPOWER J. 85, 95 n.66 (1999), available at http://www.airpower.maxwell.af.mil/ airchronicles/apj/apj99/sum99/dicenso.
Robert L. Mitchell, Reality Intrudes On the Internet, COMPUTERWORLD at 44, Sept. 3, 2001.

Uniform Computer Information Transactions Act (UCITA), 2002, available at http://www.law.upenn.edu/bll/ulc/ulc_frame.htm.

Jean Braucher, Uniform Computer Information Transactions Act (UCITA): Objections from the Consumer Perspective, 5 CYBERSPACE LAWYER

Winn Schwartau, Cyber-Vigilante Hunt Down Hackers, CNN.COM, Jan. 12, 1999, at www.cnn.com/TECH/computing/ 9901/12/cybervigilantes.idg/; see also Tedeschi supra note 4.

UNIT 17
Africa and Private Security

1.0 Introduction

There has been much written on the "scourge" of mercenaries, private military companies, and private security companies that are operating in Africa. They are blamed for instigating conflicts, for human rights abuses, for intensifying wars, for dealing in conflict diamonds, for landmines, for child soldiers, for selling small arms to warlords, even for neo-colonialism. The reality, however, is that in virtually every instance of their use on the continent, these companies and individuals that provide military services were specifically invited and welcomed by African governments. They have assisted regional stability, supported fundamental law and order, protected threatened communities of civilians, curtailed the malicious activities of insurgents, and created conditions beneficial to economic growth and political development. Thus, despite frequent vilification of companies providing military services, African governments continue to utilize or tolerate private companies filling the critical security gaps.

2.0 Objectives

This unit examines the spread, the many reasons for this; and the impact on development in Africa.

3.0 Main body

For many African citizens in the years since independence, security has been the exception, not the rule. There was a greater degree of security in the pre-independence days of the first half of the 20th century, but during that period the security was primarily designed to protect the European colonists, not the indigenous people. While we may rightly question their primary mission, colonial police and military forces were usually instilled with a strong sense of professionalism and duty by the colonial power. They were paid regularly, adequately equipped and guaranteed a pension when they retired. In the early days of independence they were critical to the stability of African states. Unfortunately, in the first years of independence African military forces

quickly declined in capability. Much of the necessary organization maintaining that professionalism ended with colonialism as their European officers and trainers as well as the essential bureaucratic structures disappeared. In most cases the former colonial powers had paid scant attention to developing any sort of long-term enduring military structure or officer class. Aggravating this trend, African leaders fearing military coups have deliberately weakened their militaries by purging them of their best officers. Post independence militaries declined quickly as a result. The tumultuous post independence years in Africa shattered any optimistic hopes that state security forces would provide stability or help to unify the new African states. Instead we have seen the decline and corruption of state security forces on the continent. Most African militaries are little more than show pieces for annual independence celebrations, and disintegrate quickly when required to perform even the simplest military task. There are many recent examples of the military ineptness common to the continent, perhaps the most obvious being the performance of the Zairian army in the final months of the Mobutu régime. Unprepared for actual combat, the army ran and looted unarmed civilians rather than face even the most feeble of attacks from the rag tag rebel factions walking west from Rwanda. Elsewhere, Zambian troops participated as a part of the UN's UNAMSIL peacekeepers in Sierra Leone.

Despite the best intentions, they arrived without even the most basic equipment, and had to be completely resupplied before they could be deployed into the field. When the RUF rebels attacked UNAMSIL in May 2000, the Zambians were quickly decimated, with hundreds being captured or killed in a matter of hours. Obviously there are a number of notable exceptions. Botswana has maintained a particularly well-equipped and professional military, and the South African military has followed a very different course. The South African National Defence Force (SANDF) continues to be the most powerful and competent military in sub- Saharan Africa. However, it is accurate to state that the vast majority of Africa's military forces are far less capable today than they were forty years ago. Blithe Western assumptions that state security forces are inherently accountable, neutral and professional simply have no relevance in Africa. State military forces are rarely passive, disinterested parties in the realm national politics. Instead, military officers have engineered the vast majority of the more than 100 coups and coup attempts that have plagued Africa since countries were given independence. Worse, due to tribal bias, shameless political manipulation, or lack of wages, African militaries have proven to be a far greater menace to the welfare of their own citizens than to the rare external threats to their states. The de-professionalizing of African militaries occurred in parallel with the disintegration of African political systems. In the hands of corrupt dictators and warlords militaries often became the primary tools of oppression. In many cases they were purged of rival ethnic groups, or deliberately marginalized by the leaders to diminish their ability to threaten the governments. As money ran out due to the gradual crumbling of national economies, the militaries became the instigators of micro-oppression

themselves as they looted their own communities to make up for the states' refusal or inability to pay even the most basic of salaries. The consequences of this degradation of African militaries are still being realized.

Legacy of the Breakdown of Security

In light of the deterioration of the general security situation in Africa, it is no surprise that foreign direct investment shuns Africa. Investors have every reason to ignore the continent and take their capital to Asia or the former communist states in Eastern Europe, and avoid the high risks and hassles of business in Africa. Most that do invest do so only in those industries with the highest returns on investment with a minimum of commitment: offshore oil, diamonds and other high-value minerals. Despite a willing and inexpensive workforce, many African governments undermine their own comparative advantages through absurd economic and tax policies, imposing pointless bureaucracy and allowing levels of corruption that make even the most determined investor blanch. Other problems such as inadequate legal systems and weak financial systems are also detrimental. But even without substantive foreign investment African countries would be considerably better off if they did not suffer from chronic conflict. It is the wars and conflicts that do the most to undermine development and prosperity on the continent. Time and again economic and social development is thwarted by military coups and civil wars. Investment or development projects designed to take years to complete may never bear fruit due to disruptions caused by armed conflicts. In many countries the pattern ensures that "long-term development" is a term only seen in academic textbooks. But it is exactly these countries suffering internal conflict are the most needy in terms of development programs. While international development agencies have often attempted to fill the void left by absent or fleeing private capital, they too are finding many countries in Africa too risky to provide effective aid. Western development agencies find their personnel are harassed and threatened by combatants, forcing many to minimize or even terminate their assistance programs. Worse, African conflicts tend to be long and brutal, meaning that the larger long-term programs are often a waste of time and resources.

For NGOs and other development organizations neutrality in the face of long-running regional or ethnic conflicts is inherently difficult and nearly as dangerous as choosing sides – unarmed Western development personnel have been robbed, raped and killed in Somalia, Sierra Leone and DRC. In fact the International Red Cross lost more people in the 1990s than in the rest of the organizations history put together. And while régimes change, international debt continues, and money stolen or squandered by previous governments is still owed by their successors, no matter how much greater the popular legitimacy of the new government. The West is loath to intervene militarily in African conflicts. Aside from the sheer danger and complexities involved, many academics and development specialists reckon that all conflicts have underlying causes that must be addressed prior to any sort of armed

intervention – no matter how horrendous the cost of delay in human terms. Others contradict this argument and point out that in too many conflicts the average age of the combatants is younger than the wars themselves, a strong sign that the underlying causes have probably been forgotten. Either way, military intervention is rarely utilized even in the most pressing cases, such as Rwanda, due directly to a lack of will in Western militaries, and a lack of capabilities in African militaries. For the West the Somali debacle dispelled any interest in becoming involved in African conflicts – no matter how desperate the need. The West's reluctance to send effective peace enforcers is likely to be further exacerbated by the new war against terrorism when there is more pressing demand for their military manpower. In the 21st Century it appears that the only competent military forces both capable and willing to intervene in African conflicts are private military companies. So instead of direct military intervention, the West has focused on addressing some of the symptoms of African wars, while doing little to end the wars themselves.

There have been a number of popular campaigns to address "Blood diamonds," landmines, and child soldiers – all worthy causes but ignoring and even marginalizing the real problem – the actual conflicts - and the shocking lack of security for the average African. The breakdown of state security has contributed to the demise of the commercial business sector. Doing business on the poorest continent in the world can be extremely expensive and dangerous due to a number of factors, including corrupt leadership happy to shakedown merchants, poorly-paid state security forces as interested in looting merchandise as protecting it, and high crime rates due to floundering economies and high unemployment. Businesses find that despite paying exorbitant taxes to the state for basic services that often do not work anyway, they also have to pay for their own security as well, adding substantially to their overhead and reducing their viability. Perhaps the most debilitating effect of the degeneration of African militaries is that usually they are the ones being called on to provide the troops for UN peace operations in African conflicts. With a depressing dearth of nations volunteering to send more competent troops, the UN is forced to rely on these inept African militaries to do their peacekeeping and peace enforcement. The problem is that no amount of good will can make up for a military that lacks training, equipment, competent officers, and logistics capability. As a result, the UN is often left with the world's least competent soldiers to do the world's most difficult peace missions, almost ensuring failures and setbacks such as in Angola and Sierra Leone. Without basic services such as logistics and transportation even the most dedicated militaries are ineffective. UN peacekeepers are not a poor man's NATO, nor should we assume they approach the capability of the preeminent military alliance. The degeneration and collapse of state security has meant citizens, businesses, and even governments have no choice but to turn to private security options. This is most obvious in South Africa, where frustration with the poor quality of the police have forced affluent home owners and neighborhoods to turn to the growing numbers of private, quick reaction

security companies. Even in the poorer neighborhoods residents often prefer to summon nongovernmental vigilante groups rather than the lackadaisical South African Police Service (SAPS). Other countries in Africa, however, are far worse off than South Africa from a security perspective, facing national wars rather than random crime. The security companies that operate those countries are appropriately more robust.

Role of Private Security

International private security services that are operating in countries suffering from serious armed conflict range from the basic private police services, to armed companies able to defend commercial installations against an organized military attack, to companies capable of carrying out offensive actions or supporting state forces engaged in regular military operations. The main thread connecting all these companies is that the key personnel are ex-military personnel from the best Western militaries – British, American, French, Belgian, Israeli or South African. They bring with them the essential skills that are critically lacking in Africa, including everything from security management, to effective logistics and supply, to basic military and police training. It is important to recognize the difference between rogue "mercenaries" and the private companies offering military services. Rogue mercenaries are individuals with military skills that are willing to work for virtually any employer, do virtually any task required, and attempt to do so with as little identification and accountability as possible. In Africa today, the majority of these rogue mercenaries are Russian, Ukrainian, Serbian, and South African. While motivations, morality and actual behavior of individuals can vary quite widely, the potential for criminal acts and abuse are enormous, whereas with legitimate, registered, monitored companies, the motivations are quite the opposite. Companies value good "names," they crave legitimacy from both their clients and their home governments, since that legitimacy is what brings contracts. Rogue mercenaries and companies providing military services may sometimes use the same personnel, but the company must be much more careful that the individual does not become involved in acts that will bring legal or financial harm or negative publicity which might cost future contracts. The UN has publicly taken an uncompromising stand against private military services. Equating them with mercenaries, they have a "Special Rapporteur on the use of mercenaries" who has grouped many private military service companies in the same condemnation he has for the rogue mercenaries.

This attempt to take the moral high road would be commendable if there was an alternative. The problem is there is nothing willing and available to take the place of the services these companies provide, so condemning the one source of effective security is clearly counterproductive and potentially harmful to international humanitarian efforts. Their removal would result in a greater breakdown in security and vastly greater human suffering on the continent. Instead the international community must look at engaging private companies to find ways of regulating and best utilizing their services. If companies are

required to live within certain regulations and guidelines in order to win lucrative UN contracts, they will do so. Private companies can do much to enhance the capabilities of indigenous militaries by providing the logistics, combat transportation, training and tactical insight that can make up for some of the past 40 years of neglect. Private companies already have worked directly with African military peacekeepers on a number of occasions to combine will with capability. Regulation means the companies are far less likely to violate international norms or laws, or engage in activities that go against the will of the international community. Actions by well-meaning NGOs and UN officials that focus on banning the trade in private military services in the face of manifest demand are in effect ignoring realities on the ground and thus encouraging unregulated actors to function beyond the ethical bounds of Western militaries. Unfortunately, much of the resentment against these private companies is driven by unfounded myths, inaccuracies and unfair assumptions. There is a need for a rational and pragmatic examination of the companies that are currently providing essential military services in African countries. And there is a distinct need to examine the security issue and better understand the dearth of alternatives to privatization, and to better appreciate the humanitarian risks of marginalizing the privatization option. What follows is an attempt to describe these companies and put them into categories that make the phenomenon easier to understand.

Self Assessment Exercise

1. In light of the deterioration of the general security situation in Africa, it is no surprise that foreign direct investment shuns Africa. Discuss.

2. What are the roles of Role of Private Security companies in development?

4.0 Conclusion

African countries have shown they can thrive in today's globalized world, given a reasonably democratic and responsive government, given a rational market based economic system, and given a basic level of safety and security for their citizens. Though they have far to go yet, some countries have proved to the world that no matter how destructive the conflict, African countries have an astonishing ability to take advantage of a globalizing world and bounce back. Because of their affordability, capabilities and flexibility, MSPs will continue to be quietly welcomed in Africa to provide the essential security needs that can support this long-term economic revitalization.

5.0 Summary

This unit highlight the spread as well as the many reasons for this; of which private companies are considered more reliable, effective, and neutral than state security services controlled by African governments. It showed that, African

states have suffered scores of coups and coup attempts from their own state forces since independence. Many state-(the military) have also been found guilty of being used to support the ethnic partiality of leaders, of horrendous human rights abuses against their own citizens, and of looting the state treasury. For modern African leaders interested in bringing stability, security and prosperity to their countries, the history of recent decades supports the rationality of decisions to increasingly privatize security, both national and commercial. Compared to conventional militaries, the record of private companies in Africa is pristine.

6.0 Tutor Marked Assignment

For many African countries in the years since independence, security has been the exception, not the rule. Discuss

7.0 References/ Further Reading

Adekeye, Adebajo and Chandra Lekha Sriram. *Managing Armed Conflicts in the 21st Century*. New York, International Peace Academy. London: Frank Cass, 2001.

Cilliers, Jakkie and Mason, Peggy (eds.) *Peace, Profit, and Plunter The Privatisation of Security in War-Torn Africa Societies*, South Africa, Institute for Security Studies, 1999. Howe, Herb. *Ambiguous Order: Military Forces in African States.* Boulder, CO:

Lynne Reinner, 2001. Mills, Greg and Stremlau, John (eds.) *The Privatisation of Security in Africa, The*

South African Institute of International Affairs, Johannesburg. South African Institute for International Affairs, 1999.

Musah, Abdel-Fatau, and Fayemi, J. Kayode, eds., *Mercenaries: An African Security Dilemma*. Pluto Press: London, 2000.

Reno, William. *Warlord Politics and African States.* Boulder, CO: Lynne Rienner, 1998.

Shawcross, William. *Deliver Us From Evil: Peacekeepers, Warlords and a World*
of Endless Conflict. New York: Simon & Schuster, 2000.

UNIT 18

Contractors as Military Professionals in Security Management

1.0 Introduction

Contractors as Military Professionals in Security Management
As of 2008, nearly 200,000 private contractors supported or supplemented military operations in Iraq, with about 30,000 of them providing security services. Today, civilian contractors working for the Pentagon outnumber uniformed forces in Afghanistan. Brooks, president of the International Peace Operations Association, the private security industry's trade organization, suggests that the booming private security industry is here to stay. Nations have employed civilian contractors to fulfil combat and combat support functions throughout history. But alarming to many observers is the rapid rise of a largely un- (or under-) controlled industry Security contractors often work side-by-side with soldiers and sometimes take on roles traditionally performed by the military.

2.0 Objectives

The unit seeks to examine the influx of private contractors and their compatibility with the strong and pervasive professional military ethos. Students are expected to:

1. Understand the motivations, values, and attitudes of individuals who sign on with private security firms
2. Shared norms, behavioural codes, professional identity, and status in relation to traditional military forces, with emphasis on military professionalism in the United States.

3.0 Main body

The Military Profession and Civilian Contractors
Over Five decades ago, Samuel Huntington and Morris Janowitz argued that military officers are professionals in the art of war and the management of violence (1963). Officers' area of expertise is in the planning, organizing, and

employment of military force. Huntington divided these tasks into two subfields: combat and command, and proficiency in "technical support (administration, comptroller, supply) and professional support (legal, religious, medical)." For Huntington, officers who mastered the technical or professional support area of military activity were not members of the military profession because their expertise was split between the management of violence and technical or job-related knowledge, the latter of which was not unique to the military.

Traditionally, it is in the technical and support categories where the employment of civilian contractors has been most prevalent. But contract employees have also penetrated into the realm of combat and command. In 2008, an estimated 30,000 contractors provided security services in Iraq. Of these, approximately three-quarters were armed, presenting the second largest armed force in Iraq, behind only the US military. At present, between 10,000 and 13,000 private security operatives are working on contracts for the Department of Defense or Department of State, constituting approximately five percent of all US-funded contractor personnel. The military's broad array of expert knowledge is organized to maximize its usefulness in tackling problems within the security arena, which is in flux at the margins as the profession expands its ambit and fends off or accedes to jurisdictional challenges from other groups, including the private sector. Nevertheless, professional military expertise still is predominant in resolving security challenges through the threat and application of organized, state-sanctioned violence at the tactical, operational, and strategic levels. Typically, in stable democratic societies, the military provides protection against external threats. Internal security is provided largely by paramilitary law enforcement groups. In post-conflict or transitional nations, however, militaries are often called upon to provide security, combat terrorism and insurgencies, and support the international community's peace and stabilization efforts.

Civilian companies also perform a wide variety of functions related to the threat or application of organized, state-sponsored force to resolve political challenges; and they are organized to effectively do so. By adopting a corporate business model, these firms are able to recruit and retain former military personnel, develop organizational frameworks within which procedures, doctrine, and innovation can be produced, and, as a result, offer an array of capabilities that cover the gamut of military services beyond mere tactical support. P. W. Singer distinguishes among three types of security businesses: military provider firms, military consultant firms, and military support firms that provide combat, training and advising, and technical support respectively. A recent study by Volker Franke and Marc von Boemcken (2009) fine-tunes this distinction, offering a five-category typology of armed operational combat support, armed security services, unarmed operational combat support, military- or security-related advice and training, and military support services. Membership in the military profession traditionally has been limited to the

uniformed personnel employed by the state. Although there is some debate regarding whether all military personnel are military professionals—be they officers, non-commissioned officers, career enlisted members, conscripts, reservists of any rank, or national guardsmen—there is a consensus that persons who utilize or manage violence as employees of private entities are not members of the military profession. When contracted to work for government agencies, the employees of private security firms lay claim to be agents of the state, albeit indirect ones. According to a recent report by the Congressional Research Service, "Conduct that violates international obligations is attributable to a State if it is committed by the government of the State or any of its political subdivisions, or by any official, employee, or agent operating within the scope of authority of any of these governments, or under colour of such authority." Former Blackwater President Erik Prince suggests such colour existed for his firm: "From the beginning, these individuals [Blackwater employees] have been bound by detailed contracts that ensure intensive government direction and control. The US government sets comprehensive standards for the selection and training of security guards. Blackwater's competitively awarded contract contains dozens of pages detailing requirements for each position and specifying hour-by-hour training for each individual' (Erik, 2008). Additionally, the revenue of these firms comes primarily from government sources. The Congressional Budget Office estimates that direct US government spending on private security services in international locales was $6 billion to $10 billion over the 2003-2007 period with $3 billion to $4 billion spent in Iraq. Such expenditures rival the defence budgets of many nations. Another key aspect of the military profession is its vocational nature; its members are not primarily motivated by material rewards. Huntington argued that:

> *The officer is not a mercenary who transfers his services wherever they are best rewarded . . . Clearly he does not act primarily from economic incentives. In western society the vocation of officership is not well rewarded monetarily. Nor is his behaviour within his profession governed by economic rewards and punishments . . . . The motivations of the officer are a technical love for his craft and the sense of social obligation to utilize this craft for the benefit of society*

Charles Moskos suggested that vocations motivated by economic rewards are occupations rather than professions. Military professionals receive compensation that is a function of pay grade, much of which is deferred or in the form of subsidies rather than cash for service. Clearly, by this standard, mercenaries "who fight for employers other than their home state's government [and whose] motivation for fighting is economic gain" fall outside of the military

profession. Many have argued that the prospect of extraordinary monetary gain serves as a central motivator for individuals to sign on with private security firms and engage in what we term in this context the "securitized management of violence." Indeed, private security firms pay considerably higher wages than the military at the comparable skill level and grade.

In modern democracies, the military profession derives legitimacy from its license to implement the state's monopoly on the legitimate use of force in combination with its subordination to civilian command and control. For Huntington, submission of the military to civil authority is the sine qua non of military professionalism. Civilian professionals, by contrast, gain legitimacy through commitment to their employer's or client's interests. As employees of private firms, security contractors at best have divided loyalties, answering as they do to their employer for their performance rather than directly to their client.

Because the military works exclusively for the state, "the commitment of the professional to the client is thus changed to 'loyalty to the nation and its value-system.'" In democracies, "society insists that the management of violence be utilized only for socially approved purposes." Because private security firms need not answer directly to the polity for their performance, only their shareholders and management, there are few guarantees that they will utilize violence only for the purposes and in the ways that would be socially sanctioned by the citizenry. This lack of accountability has been perhaps the key source of unease about the behaviour of private security firms in Iraq and Afghanistan, particularly when incidents that involve significant harm to non-combatants come to light. But it is not only this exclusivity arrangement based on democratic norms and values that brings legitimacy to the profession of arms. There is also a utilitarian calculus derived from political effectiveness and economic efficiency that legitimizes the military as a unique social institution. Traditionally, a standing military has been viewed as the most efficient and effective solution to national security threats and challenges. This view has been, perhaps, the primary driver of acceptance of militaries throughout history, accounting (in the American case) for the high esteem in which military men were held after the Second World War and Operation Desert Storm and the low esteem in which they were held during and following the Vietnam War. In other words, effectively performing its primary mission constitutes the "special social responsibility" from which the military profession derives its legitimacy.

Security contractors also gain legitimacy by being politically effective and economically efficient. Singer argues that the opaqueness of their relationship with political authorities can increase their political utility by providing services that states would rather hold at arm's length or hide from public view. Contractors also gain legitimacy from their supposed cost effectiveness. Indeed, the claim that private-sector actors are more efficient and effective than

those employed by the public sector has been the primary means of legitimating the privatization movement. Finally, members of the military profession share a corporate identity honed by their common experiences in training, education, and practice, as well as a command structure that controls entry into the profession, establishes polices and standards of competence, and prohibits members from practicing outside of its legitimate ambit. As Sir John Hackett wrote, "The essential basis of the military life is the ordered application of force under unlimited liability. It is the unlimited liability which sets the man who embraces this life somewhat apart. He will be (or should be) always a citizen. So long as he serves he will never be a civilian." Military members' behaviour is regulated by the *Uniform Code of Military Justice* every moment that they are on active duty and even after they retire from active duty (so long as they do not resign their commission and elect to accept retirement pay). Thus, the profession continues to shape its members' attitudes and conduct throughout their lifetime, thereby reinforcing its corporate identity.

A case could be made that civilian employees of private security firms also share an identity with the military. Many employees are former members of the military and some are retirees who retain their commission and theoretically could be recalled to active duty. They may belong to the private associations of their former service and feel a kinship to their active-duty colleagues. Apart from this military kinship, some firms quite carefully recruit, train, and even indoctrinate their employees to inculcate a professional identity. On the other hand, there is a prima facie case to be made that employees of the security industry do not and likely cannot share a corporate culture given the diversity of firms, clients, and the eligible labour pool. "It is estimated that some 50 private security contractors employing more than 30,000 employees are working in Iraq for an array of clients, including governments, private industry, and international organizations such as the United Nations." There are a multitude of private security firms. Many are characterized by a cadre structure with a relatively low number of full-time employees and a reservoir of expertise that can be called upon on a contract basis. Such a structure would appear to undermine any attempt to indoctrinate these employees or to foster a professional, corporate identity. Franke and Boemcken argue that the nature of the tasks to be performed encourages small-group cohesion but not necessarily the development of a distinct professional identity. Instead, contractors of similar background tend to cluster together, such as those with law-enforcement or special-operation experience, and are wary about interacting with people from other career fields. Unlike the military, there is no enforced conformity in all aspects of life for civilian contractors over an extended period of time that could forge a common identity. Civilian contractors have many of the traits of military professionals; they possess expert knowledge to manage organized violence, apply it within the military's jurisdiction, are primarily agents of the state although not directly employed by it, and gain legitimacy through provision of effective solutions to their client's problems. On the other hand, they are not uniformed agents of the state, are motivated by

compensation rather than social obligation, and have divided loyalties and a questionable corporate identity.

Self Assessment Exercise
The military is a unique social institution of security. Discuss.
Why do Military professional than other private security personnel?

4.0 Conclusion

Given that armed contractors possess expertise in the application and management of organized violence, have acted as agents of the US government, and provide cost-effective solutions to problems within the traditional jurisdiction of the military profession, they may have a claim to status as military professionals. Indeed, the fragmented nature of the industry, its multitude of firms, heterogeneous labour pool, and difficulties in forging a common corporate identity through coherent and consistent indoctrination, training, and educational experiences suggests, however, that armed contractors should at best be considered to be members of a semi-profession. Incorporating contractors into the military profession would dilute its corporate identity, its dedication to a common good, its ability to control members' entry, promotion, and exit, and would cripple the legitimacy of the armed forces as clearly demarcated and legal agents of the state.

5.0 Summary

This section delineates the traits of the military profession and assesses the degree to which civilian contractors possess these traits. Issues relating to the military as a profession were discussed. Answers were provided regarding military as professionals.

Tutor Marked Assignment
Explain the concept of uniform code of military justice and how it regulates behaviour.

Military members' behaviour is regulated by the *Uniform Code of Military Justice.*

6.0 References/ Further Reading

Charles C. Moskos, Jr., "From Institution to Occupation: Trends in Military Organization," *Armed Forces and Society*, 4 (Fall 1977), 43.

Deborah D. Avant, *The Market for Force: The Consequences of Privatizing Security* (New York: Cambridge Univ. Press, 2005), 47-49.

Erik D. Prince, "How Blackwater Serves America," *The Wall Street Journal*, 16 December 2008, A23.

Jennifer K. Elsea, Moshe Schwartz, and Kennon H. Nakamura, *Private Security Contractors in Iraq: Background, Legal Status, and Other Issues* (Washington: Congressional Research Service, updated 29 September 2008), 14, note 52.

John Hackett, *The Profession of Arms* (London: Times Publishing Co., 1963), 63.
Samuel P. Huntington, "Power, Expertise, and the Military Profession," *Daedalus*, 92 (Fall 1963), 785.

Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* [Cambridge, Mass.: Belknap Press of Harvard Univ. Press, 1957], 12.)

Samuel P. Huntington, *The System of Professions* and Steven Brint, *In an Age of Experts: The Changing Role of Professionals in Politics and Public Life* (Princeton, N.J.: Princeton Univ. Press, 1994).

Volker Franke and Marc von Boemcken, *Attitudes, Values, and Professional Self Conceptions of Private Security Contractors in Iraq: An Exploratory Study* (Bonn, Germany: Bonn International Center for Conversion, 2009), 7-9.

UNIT 19

Community Policing — Working Together to Prevent Crime

1.0 Introduction

Since the mid 1980s, the concept of 'crime reduction through community partnership' has continued to grow in popularity. At a time when traditional policing activities failed to deliver tangible reductions in local crime rates, this significant shift in the traditional policing paradigm led to the increased use of one important policing strategy: community policing. However, 'community policing' is a very broad term often used to describe many aspects of the process by which the police engage with the community in the prevention of crime. At its core is the recognition that by working with the community, law enforcement agencies can find local solutions to local problems. Engaging the community in crime reduction and prevention allows a more targeted approach to local priorities by empowering the community to identify and respond to local concerns. The benefits can be widespread, from improved police–citizen relations to decreases in the fear of crime.

2.0 Objectives

This unit examines community policing in practice, with a particular focus on both national and international research into its effectiveness. Students are expected to know the benefits and pitfalls of current community policing initiatives outline possible future directions for communities and crime prevention.

3.0 Main body

Community policing has emerged in as an innovative law enforcement response in dealing with, and preventing crime. It is a term often used to describe the process of engagement between the police and community and at its core is the recognition that by working with the community, law enforcement agencies can find local solutions to local problems. Community policing is thought to have gained momentum for a variety of reasons, not the least of which was the general community dissatisfaction with traditional law

enforcement practices and the demand for greater police accountability for increasing crime rates. Community policing recognises that community members can work together with law enforcement agencies and play an active role in reducing local crime (Segrave and Ratcliffe 2004, p. 2).

The development of a clear definition of community policing is hindered by the fact that most police services, both nationally and internationally, label almost any 'non-reactive' police strategy as a community policing initiative (Edwards 1999, p. 76). It is recognised that a unanimous definition of community policing has not yet been established (Fielding 1995) as it is conceptualised differently by many individuals (Cordner 1998). That being said, the fundamental cornerstone of community policing is in forming a workable partnership with the community, where the community plays a more proactive role in helping develop crime prevention strategies (state the general role of the community) (Peak and Glensor 1999 cited Segrave and Ratcliffe 2004). Cordner (1998) determined that there are essentially four facets of community policing: The *philosophical*, where the community's role is fundamental and the police's role is expanded from traditional policing duties (Bennet 1998); the *strategic*, where ideas from community policing are developed into strategies for practice (p. 48); the *tactical*, which focuses on the implementation of the strategies developed; and the *organisational*; where the support offered at an organisational level should be encouraged to promote community policing.

3.1 Perceived benefits

Advocates for community policing have highlighted many reasons why community policing is beneficial to society. These arguments were broken down into three areas by Segrave and Ratcliffe (2004):

Community-specific advantages

- Mobilisation and empowerment of communities to identify and respond to concerns
- Improved local physical and social environment
- Increase in positive attitudes towards police
- Reduced fear of crime.

Police-specific benefits

- Improved police–community relationship
- Improved community perception of police 'legitimacy'
- An increase in officer satisfaction with their work.

Shared benefits

• A decreased potential for police–citizen conflict

• A reduction in crime rates

• A better flow of information between the police and community

• Better implementation of crime prevention and crime control activities, as a result of both parties working towards shared goals.

Not all community policing initiatives will achieve each and every benefit listed here and part of the problem of documenting success is that researchers rarely find that the strategies *only* have positive effects. Internationally, successful implementation of community policing has been documented, although the results are rarely black and white. Two specific examples of the ambiguity of community policing success can be found in a United States experiment and in an evaluation of Hong Kong's implementation experiences. Community policing in Hong Kong has been found to be a positive step in improving police–public relations and engaging the public in crime prevention; however, the Hong Kong police were found not to promote greater community–police partnerships, and did not encourage the community to help develop law and order strategies, one of the common goals of community policing. A US community policing study by Hawden (2003) assessed that the community's opinion of the police improved when police were more visible, however it did not increase their perception of police effectiveness.

3.2 Pitfalls

As an increasing number of studies are conducted on community policing, the pitfalls and challenges of implementing such strategies are becoming more evident. As community policing grows in popularity and implementation, studies have increasingly found that community policing is not a panacea that is easily implemented with immediate success. Related problems can manifest in three different areas: within the police service; within the community; and in the implementation of community policing initiatives.

3.3 Within the police service

Many studies on the police services in home and overseas have documented the challenges faced when implementing community policing. These include barriers from within the police organisational structure and the organisational climate, where the absence of strong leadership and encouragement in community policing strategies can negatively impact on community policing practices (Robinson 2003). Whereas police leadership in community activities can be needed and sought by its members, there are some less noticeable hindrances to implementing community policing. Police may also be reluctant to make community policing a priority due to the perception that community

policing is distinct from other ‘police work,’ thus reinforcing the notion that it is not ‘real’ police work.

3.4 Within the community

There can also be quite a romanticised perception that the community will be eager to embrace community policing methods. For some, community members are reluctant to seek and develop a sustainable partnership with law enforcement and communication constraints can often hinder community policing success, especially in areas with minority and special needs groups (Schneider 1998). Research has also found that community and police cohesion on the problems and solutions existing in a community is not necessarily present, and can be dominated by minority stakeholders .

3.5 Implementation

There is no uniform model of community policing, and adopting the western model can pose problems in developing countries such as low levels of professionalism, disrespect for law enforcement, lack of community organisation and other contextual factors. Community policing in Nordic countries was found to have limited success, and was abandoned in Finland and Norway. The initiative’s failure was explained as the result of an already high perception of public safety, lack of citizen association of police visibility and safety and traditionally the lack of Nordic citizen involvement in its welfare state (Holmberg 2005). This demonstrates that the practice of transplanting community policing initiatives without accounting for different cultural contexts can prove to be a major hurdle in successful community policing implementation.

Self Assessment Exercise

What does community policing entail?

4.0 Conclusion

Overall, the challenges in implementing community policing vary from nation to nation — even state to state. Law enforcement agencies should not expect immediate results from implementing new community policing initiatives. Community policing requires significant financial and organisational investment, and agencies wishing to implement such practices should base actions on proven successful methods and only if they are able to be adapted to suit the local context .

5.0 Summary

In their overview of community policing, Segrave and Ratcliffe concluded there were three continuing challenges remaining for community policing implementation: building community partnerships, which in are often more challenging to develop than police perceive; making community policing an

integrated approach to policing with other complementary policing strategies (e.g. problem-oriented policing and intelligence-led policing); and the need to strengthen research into community policing strategies to determine its effectiveness as a policing tool. In this emerging era of community policing, it is rarely considered — or perhaps less widely advertised — whether the increase in community contact by the police can have adverse affects on the police. A challenge faced by those implementing community policing is the increase of civil litigation against police. Some researchers have hypothesised that due to heightened community contact by the police via community policing initiatives, police have greater exposure to litigious circumstances (Stubbs 1992; Worrell and Marenin 1998).

5.0 Tutor Marked Assignment

What are the perceived benefits of community policing and the challenges therein?

6.0 References/ Further Reading

Bennet T 1998, 'Police and public involvement in the delivery of community policing', in ed. J P Broudeur, *How to recognize good policing: Problems & issues*, Sage & Police Executive research forum, Thousand Oaks.

Bohms R M, Reynolds K M & Holmes S T 2000, 'Perceptions of neighbourhood problems and their solutions: Implications for community policing', *Policing: An international journal of police strategies and management*, vol. 23, no. 4, April, pp. 439-65.

Brogden M 2004, 'Commentary: community policing: a panacea from the West', *African Affairs*, vol. 103, no. 413, October, pp. 635-49.

Cordner G 1998, 'Community policing: Elements & effects', in eds Alpert & Piquero, *Community policing: Contemporary readings*, Waveland Press, Illinois.

Davis R, Henderson N & Merrick C 2003, 'Community Policing: Variations on the western model in the developing world', *Police practice and research*, vol.4, no. 3, pp. 285-300.

Edwards C 1999, *Changing police theories for 21st century societies*, Federation Press, Sydney.

Fielding N 1995, *Community policing*, Clarendon Press, Oxford.

Giacomazzi A, Riley S & Merz R 2004, 'Internal and external challenges to implementing community policing: Examining comprehensive assessment reports from multiple sites', *The justice professional*, vol. 17, no. 2, June, pp. 223-38.

Hawden J 2003, 'Police-resident interactions and satisfaction with police: An empirical test of community policing assertions', *Criminal justice policy review*, vol. 14, no. 1, pp. 55-74.
Holmberg L 2005, 'Policing and the feeling of safety: the rise (and fall?) of community policing in the Nordic countries', *Journal of Scandinavian studies in criminology and crime prevention*, vol. 5, no. 2, pp. 205-19.

Lo C W H –C & Chun-Yin A 2004, 'Community policing in Hong Kong: Development, performance and constraints', *Policing: An International Journal of Police strategies and management,* vol. 27, no. 1, pp. 97-127.

Long J, Wells W & Leon-Granados W D 2002, 'Implementation issues in a community and police partnership in law enforcement space: lessons from a case-study of a community policing approach to domestic violence', *Police practice and research*, vol. 3, no. 3, pp. 231-46.

Peak K & Glensor R 1999, *Community policing & problem solving: strategies & practices*, 2 edn, Prentice Hall, New Jersey.

Robinson A L 2003, 'The impact of police social capital on officer performance of community policing', *Policing: an international journal of police strategies and management*, vol. 26, no. 4, pp. 656-89.

Schneider S R 1998, 'Overcoming barriers to communication between police and socially disadvantaged neighbourhoods: a critical theory of community policing', *Crime law and social change,* vol. 30, no. 4, pp. 347-77.

Segrave M & Ratcliffe J 2004, Community policing: A descriptive overview.

Stubbs J 1992, *Complaints against police in New South Wales,* NSW Bureau of Crime Statistics and Research, Sydney.

Worrell J L & Marenin O 1998, 'Emerging liability issues in the implementation and adoption of community-oriented policing', *Policing: an international journal of police strategies and management*, vol. 21, no. 1, pp. 121-36.

UNIT 20
Policing Terrorism: A Threat to Community Policing

1.0 Introduction

The introduction of community policing has been heralded as the most significant and progressive change in policing philosophy and there are good reasons for this claim. Having a distinctly proactive emphasis, community policing has proven to be a dramatic improvement to the traditional model of policing that is essentially reactive. Characteristically, traditional policing almost invariably depends on a paramilitary structure that tends to distance police from the rest of the community. Community policing, on the other hand, relies on a cooperative community arrangement which when working effectively reduces not just the incidence of crime but also the fear of crime.

2.0 Objectives

This unit seeks to explain the growing trend of forceful policing after the event of September 11 in the United States and in the war against terrorism in every nation.

3.0 Main body

It has been frequently said that the terrorist events of *September 11* have changed the world forever. To some observers, so too has the public profile of policing. In many countries now there have been signs of police reverting to (or in some cases simply reaffirming) paramilitarism, which is more in line with the traditional model of policing and clearly at odds with community policing. The threat of terrorism that exists today will test the resolve of police commissioners who choose to retain community policing as a dominant policing philosophy. In this new environment, there is no doubt the effectiveness of community policing will be challenged and some will rationalize it away as being too soft to match the so-called ‘war against terror.’ While some police forces/services will continue to rely on the community policing model, others will be tempted to return to a traditional model and

varying degrees of paramilitarism. Williams (2003, p. 119) notes already in the USA, that the 'effort to incorporate the community policing model into traditional policing operations is faltering.' Another pressure on community policing is governmental influence: in the context of the drive for effectiveness and efficiency and the election value of law and order, some governments will promote the view that police should concentrate on core business which will be interpreted as requiring police to focus on crime fighting. In this paper I examine, then contrast traditional policing with community policing and in particular critique the paramilitarism of the former to challenge its relevance to policing generally.

Another major consideration in the maintenance of community policing as a dominant philosophy is the prevailing police culture. I comment on the cultural change that was needed in the transition to community policing and while many police forces/ services have ostensibly managed the cultural change to accommodate community policing I warn of the underlying tension that probably still exists in police culture which is likely to prefer the traditional model of policing. Put another way, operational police are likely to consider community policing inappropriate to police terrorism. Consequently, for those police commissioners who would seek to retain community policing, this presents a real challenge especially in a climate which tends to demand a more visible and aggressive force against terrorism. Though trite, it has been frequently pointed out that police alone cannot successfully achieve crime control and that the support of the community is critical—the same principles clearly apply to the prevention of terrorist acts (and prevention should surely be the emphasis). While threats against national security have justifiably shifted the focus of policing priorities to meet this critical demand, I argue that any shift in policing strategies overall should be in emphasis only and not an abandonment of community policing and a total return to the paramilitarism of the traditional model. The shift in focus to counter terrorism will quite rightly involve placing more resources in paramilitary units and providing front-line officers with the necessary skills. However, to do so by abandoning community policing as an overall philosophy will be, counterproductive since it takes away the critical facility of prevention and community cooperation which are inherent in community policing. The two policing philosophies of paramilitarism and community policing can (and in this current environment should) coexist, but under the umbrella of community policing.

3.1 Transition from Traditional/Paramilitarism to Community Policing

For much of the developed world, the origins of the modern police service can be traced to the creation of the Metropolitan Police in London in 1829 (Reith, 1975). Introduced by Sir Robert Peel, the Bill to proclaim the *Metropolitan Police Act* in England was accompanied by a set of principles for policing which I consider to have equal relevance today. The organizational structure and managerial philosophy that accompanied the establishment of this earliest police organization were consistent with the literal definition of paramilitarism.

The paramilitary stamp was firmly put in Peel's police, evidenced by the fact that: (i) Peel ensured the police must be stable, efficient, and organized along military lines (Waters & McGrath, 1974, referred to by Auten, 1981); (ii) there was virtually no organizational model other than the military to emulate; and (iii) there was a conscious decision that the inaugural leader of the Metropolitan Police should be a military person (Auten, 1981). In fact, the authors of the first manual of instruction adapted their text from the 1803 military manual of the Irish Constabulary Police, entitled *Military training and moral training*. The move from a traditionally reactive, action-oriented style of policing to a service oriented community policing model, which occurred over the last three decades, has arguably been the most significant positive change in policing philosophy. To Bayley (1994, p. 104), for example, 'community policing represents the most serious and sustained attempt to formulate the purpose and practices of policing since the development of the 'professional' model in the early twentieth century.' The introduction of community policing followed what were seen as the limitations of traditional policing and the need for change.

Moore (1994, p. 285) neatly summarizes this: [Referring to the Community Policing Movement] It is not hard to understand the attraction of the new ideas about policing. They seem to recognize and respond to what have come to be seen as the limitations of the 'reform model' of policing: its predominantly reactive stance toward crime control; its nearly exclusive reliance on arrests as a means of reducing crime and controlling disorder; its inability to develop and sustain close working relationships with the community in controlling crime; and its stifling and ultimately unsuccessful methods of bureaucratic control. In contrast the new ideas point to a new set of possibilities: the potential for crime prevention as well as crime control; creative problem solving as an alternative to arrest; the important of customer service and community responsiveness as devices for building stronger relations with local communities; and 'commissioning' street-level officers to initiate community problem-solving efforts. (Sparrow et al., 1990) Researchers and commentators have found police services that have embraced community policing refer to its cornerstone as the collaborative partnership between the community and the police, engaged in a process that identifies and solves problems of crime and disorder. While there appears to be no single definition of community policing, Oliver and Bartgis (1988, p. 491) note there is a constant theme in the literature:

> The majority of definitions focus on an increase in police and community interaction, a concentration on 'quality of life issues,' the decentralization of the police, strategic methods for making police practices more efficient and effective, a concentration on neighbourhood patrols, and problem-oriented or problem-solving policing.

Public attitudes to the police will also be a determinant in the success of community policing. A hostile or fearful community, for example, will be disinclined to cooperate with police. Police, as Roberg (1994, pp. 251–252) notes, may not be unduly concerned about that since many line officers have been 'recruited, trained and socialized in a traditional law enforcement orientation and may have a stake in preserving the status quo.' Oliver and Bartgis (1988) found line officers had the capability to ignore, circumvent, or sabotage the desires and expectations of the community. Since the transition from traditional policing required a substantial change in police culture it is appropriate to examine what the cultural traits of traditional policing are, and how, or to what extent do they contrast with those of community policing?

Police Occupational Subculture: A Bias Towards Traditional/Paramilitary Policing?

There is no doubt that given the extensive authority and discretion held by police that they have the potential to have a dramatic impact on the lives and liberties of citizens. Reflecting on the importance of maintaining a keen interest in policing, Van Maanen (1978, p. 311) thought policing to be 'possibly the most vital of our human service agencies … too important to be taken-for-granted, or worse, to be ignored.' It certainly follows, therefore, that the ideology, values, principles, and preconceptions which are generally held by police and which consequently determine police culture, are of critical consideration. Unlike most other vocations, discretion in policing is strongest at the lowest level of the organization and while decisions to arrest are open to scrutiny, *most* police decisions involve actions other than arrest, and are therefore, largely without scrutiny or control. Occupational police culture has been the subject of regular examination by many theorists, the most prominent of them being Skolnick (1966, 1985) in the USA; Cain (1973) and Reiner (1992) in Britain; and Chan (1996, 1997, 1999) and Prenzler (1997) in Australia. Many definitions and descriptions of police culture have followed which include: 'developed recognizable and distinct rules, customs, perceptions and interpretations of what they see, along with consequent moral judgements' (Skolnick & Fyfe, 1993, p. 90); 'an identifiable complex of common culture, values, communication symbols, techniques, and appropriate behaviour patterns' (McBride, 1995, p. 214); and Reiner (1992, p. 21) equates it with the 'values, norms perspectives and craft rules' that inform police conduct. Skolnick (1966) refers to the 'working personality' of police which is associated with the police task and is characterized by suspiciousness, internal solidarity, social isolation, and conservatism. Reiner's (1992) subsequent work resulted in similar conclusions. He found that a 'central feature of cop culture is a sense of mission [and that to police themselves] policing is not just a job but a way of life with a worthwhile purpose' (Reiner, 1992, p. 111). He also noted that the 'core of the police outlook is this subtle and complex intermingling of the themes of mission, hedonistic love of action and pessimistic cynicism' (p. 114).

Pertinent to this subjectr, he found that ‘most policemen are well aware that their job has bred them an attitude of constant suspiciousness which cannot be readily switched off [accompanied by a] marked internal solidarity, coupled with social isolation’ (pp. 114, 115). These findings have been supported to varying degrees by Fitzgerald (1989). The most interesting aspect of the general findings about operational police culture, as outlined above, is that when summarized they are almost diametrically opposite to what have identified as the appropriate/ideal characteristics of a community police officer which include: a genuine belief in community consultation and problem solving; commitment to the notion of equal partnership with the community; creativity and innovation; freedom to exercise discretion at the lowest level of policing; excellent communication skills so as to be able to develop a rapport with the community, and in turn, win trust and respect. Table 1 contrasts these ‘ideal’ characteristics for a community police officer with the cultural traits identified in research. One suspects, however, the research findings are not as stark as they appear since they tend to ignore the positive aspects of police culture. Chan (1997) in making this point believes police culture has become a convenient label for a range of negative values, attitudes, and practice norms among police officers; and notes that judicial and scholarly references to police culture have been almost universally pejorative. James and Warren (1995, p. 4) suggest this to some extent can be explained by the fact that:

The origins of cultural explanations for police behaviour can be traced to attempts by sociologists in the 1960’s to explain an enduring anomaly in policing: the breaking of rules by the people whose primary occupation and sole purpose is to enforce rules.

Table 1 Competing Police Profiles

‘Ideal’ profile for community police officer	Research profile for operational police
Commitment to community consultation and problem solving.	A sense of mission about police work but a distancing from the rest of the community.
Open and accessible in the provision of a service.	Suspiciousness.
Creative and innovative in promoting solutions to problems and crime prevention.	A pragmatic view of police work which discourages innovation and experimentation.
Freedom to exercise discretion at the lowest level of policing so as to incorporate a problem-solving mentality as an alternative to arrest.	A preference for action orientation and arrests.
Excellent communication skills so as to be able to develop a rapport with the community, and in turn win respect and trust.	An isolated social life coupled with a strong code of solidarity with other police officers. A cynical or pessimistic perspective about their social environment.

Despite studies repeatedly showing that most police work involves situations where no crime has occurred, there is a preference by police for action orientation rather than service provision At the same time, some governments place a heavy reliance on response-based performance measures such as the

number of arrests as indicators of police effectiveness since quantitative targets are easy to define and present a more convenient solution to political demands.

Subculture and its Alignment to Models of Policing

Traditional policing which places a heavy emphasis on paramilitarism and community policing which is founded on a more democratic model give rise to quite different cultures. Many police services have successfully managed the cultural transition from action to service orientation that accompanied the shift from the traditional to the community policing model, while others have experienced resistance arising from the preference within police culture for crime fighting rather than problem solving. This tension becomes pertinent in the light of outside pressures today such as the imperative to address terrorism and national security. Some services have preferred to retain the traditional model of policing, albeit in modified form. As police services around the world address national security, an examination of the differences in police culture that tend to be aligned to traditional vs. community policing is appropriate.

Craft or Professional Culture?

Proponents of traditional policing tend to regard policing as a craft or trade, which is best, learned 'on the job.' It is assumed in this model that it is best to have the majority of training/mentoring undertaken by experienced officers in a master/apprentice arrangement. Certainly in former times, 'outside' help was neither requested nor respected. For community policing an open approach is adopted for recruitment, training, and development, interpreted by some as a move towards policing being a 'profession.' What profession means is, of course, open to different interpretations but has generally thought within policing circles to include the development of a body of knowledge, a strict code of ethics, and working to values rather than rules. In cultural terms, with traditional policing there is a strong preference for the status quo, where seasoned officers perpetuate existing culture resulting in insularity and an 'us' (police) and 'them' (community) mentality. With community policing a culture develops which places a great deal of reliance on community expectations and a willingness to join with, and learn from, experts outside policing.

Paramilitarism or Democratic Managerial Culture?

Traditional policing, as Auten (1981, p. 68) notes, promotes a paramilitaristic managerial style which will exhibit at least some of the following characteristics:

● A centralized command structure with a rigidly adhered to chain of command;

● A rigid superior–subordinate relationship defined by prerogatives of rank;

● Control exerted through the issuance of commands, directives, or general orders;

- Communications being primarily vertical—from top to bottom;
- Initiative being neither sought nor encouraged;
- An authoritarian style of leadership;
- An 'us–them' division between senior officers and the rest; and
- Discipline being rule based and punitive.

Traditional policing relies heavily on these characteristics not only to ensure effectiveness and efficiency through command and control but also to maintain discipline. Proponents of community policing have never denied the need for command and control but point out that occasions where it is required are relatively few and that its emphasis in the traditional model is disproportionate and counterproductive. With community policing there is a more democratic style of management which relies on personal credibility rather than rank-based authority. With the traditional model, the culture typically manifests an expectation of unquestioned acceptance of direction from a senior officer and one-way communication. This culture assumes that subordinate ranks need to be told what to do, that rank decides the 'right' decision and those down the ladder will have little to offer. The more democratic style in community policing allows empowerment to be devolved to the lowest possible level so as to allow greater decision-making at the operational level. This gives rise to a culture which allows initiative and problem solving. The culture inherent in community policing also recognizes the need for command and control for those occasions where it is required and will adapt for the occasion.

Authoritarian or Problem-Solving Culture?

With traditional policing there is an emphasis on arrests and the strict enforcement of laws, little consideration of prosecutorial discretion, limited interest about the causes of crime, less emphasis on crime prevention, and a general assumption that police will know what is best for the community at large. Community policing on the other hand is founded on the primacy of crime prevention and a conscious commitment to joining with the community in problem solving. The cultural expectations for these two models are dramatically different. Skolnick (1966) and Reiner (1992) whom I refer to above, found with traditional policing that police culture demonstrates a tendency for action orientation and a general distancing from the community. With community policing the culture will show a tendency for openness, innovation, community interest, service orientation, and a spirit of problem solving.

Compliant or Adaptive Culture?

The traditional model of policing tends to have: (i) a centralized structure with headquarters as the source of orders, rules, and regulations; (ii) standardization

and uniformity; (iii) measurement of performance based on quantitative criteria such as the number of arrests; (iv) excessive specialization; and (v) a narrow definition of the duties of a patrol officer being limited to attending complaints and working to predetermined rules and practices. This relatively compliant model meets with problems when confronted with situations not readily covered by existing directives, general orders, or policy and procedure. Community policing adopts a more adaptive approach through (i) a decentralized structure with the aim to bring the police closer to the community with headquarters being the source of support direction, norms, and values; (ii) encouragement and support for flexibility; (iii) measurement of performance-based not just on quantitative but also qualitative criteria such as the achievement of community goals or solving problems; (iv) a move from specialization to a balance between versatility and specialization; and (v) the patrol officer is a generalist responsible for attending complaints, solving problems, activating the community, preventing crime, and undertaking preliminary crime investigations, where the discretionary powers of the patrol officer are recognized and developed. With traditional policing, officers are trained to work to established rules and regulations. The culture, therefore, tends to be regimented to act on direct orders with the assumption that the rank-based authority ensures not just compliance but also efficiency and effectiveness. With community policing there is a more flexible structure and a culture develops which is more conducive to recognizing that there is usually no single solution to problems/issues and that by recognizing the valuable contribution from those in the field a more practical resolution is likely. At an operational level, officers will have more confidence to deal with community issues.

Recognizing the Appropriate Model

A shift from traditional to community policing needs a major transition in both managerial and cultural terms. Plainly the characteristics of traditional policing are not suited to community policing. Table 2 highlights differences between the two models. As the ‘world changed’ after *September 11*, the question that now has to be asked is, ‘Are we seeing a reversion to the paramilitarism of the traditional policing model or has there been merely a shift in priorities?’

The Threat of Terrorism and Impact on Community Policing

Prior to *September 11*, many countries in the developed world had lapsed into a laissez-faire approach to national security. The terrorist attacks in the USA on domestic soil would bring that complacency to a dramatic end, and priority for ‘homeland security’ would become a catch cry, not just in the USA, but also in many countries. This required strategic consideration about how military and civil services would reconfigure to address this fresh challenge. While defence forces would obviously feature in the reassessment, policing would also have increased responsibilities. In many countries the changes have been dramatic and have plainly been much more than tightening up existing practices. De Guzman (2002, p. 8), for example, described the reaction in the USA as the

'fortification' of the country. Policing across the world, to the average observer, became visibly different. It was not just the fact there were more police about, but police had also assumed a more aggressive style of dress and manner.

Table 2 Transitions between Traditional and Community Policing

Traditional policing and links to paramilitarism[a]	Community policing and democratic management	Culture—contrasting and comparing
Policing as a craft Traditionally policing was regarded as a craft/trade which was best learned 'on the job.'	*Policing as a profession* There has been a conscious drive for policing to be accepted as a 'profession.'	*Culture developed on the job* With traditional policing there is a strong reliance on the status quo and learning from experienced officers. With community policing a more 'open' culture develops which places a great deal of reliance on community expectations.
Paramilitary management style Traditional policing incorporates a managerial style which is based either entirely on military lines or at least draw on their principles.	*Democratic management style* While command and control is necessary, these situations are relatively few and management allows contributions from all ranks as to how the job is done.	*Empowered or disempowered culture* A paramilitary culture assumes that authority is linked to rank. With a democratic style of management the culture is one which empowers all officers.
Authoritarian approach to policing Traditional policing promotes strict enforcement of laws, little concern about the causes of crime, limited prosecutorial discretion, and there is less emphasis on preventing crime.	*Problem-solving approach to policing* Here there is an understanding what causes crime and there is a conscious commitment to joining with the community to prevent crime.	*Linking culture to the philosophy* In traditional policing there is a tendency for authoritarianism, defensiveness, cynicism, and action orientation which together result in a general distancing from the community. In community policing the culture is open, consultative, and geared to solving problems.
Inflexible structure In the traditional model, there tends to be a rigid, centralized bureaucracy with officers working to predetermined rules and practices.	*Flexible structure* Community policing devolves authority and decision-making which encourages initiative. Officers work to values and standards.	*From compliant to adaptive culture* With traditional policing, the culture tends to be regimented and compliant. Community policing is adaptive recognizing that there is usually no single solution to problems/issues.
Blame culture The paramilitary model of policing assumes that police officers will inevitably do something wrong and when they do they should be punished.	*Learning culture* A learning culture recognizes the failure of the punitive model and educates/corrects minor and understandable breaches rather than punish.	*From institutional to personal discipline* The punitive model creates apprehension, anxiety, defensiveness, and denial. An 'us–them (management)' culture results. In a learning culture officers work to values and minor breaches are regarded as curable mistakes—a move from threat to incentive.

Table 2 *Continued.*

Traditional policing and links to paramilitarism[a]	Community policing and democratic management	Culture—contrasting and comparing
Insularity and defensiveness In traditional policing there is a tendency towards the notion that police are the only ones who knew anything about policing. Academics or other commentators are not appreciated.	*Openness and consultation* In community policing other expert advice is invited and individual police contributions are considered worthwhile.	*Move towards transparency* With traditional police there was a defensive culture—a tendency towards craft secrecy. Inherent in community policing is that police are part of the community and a desired culture is one which recognizes and works to a model that allows the public to know how and why the police operate the way they do.

[a] In listing the characteristics of traditional policing and the link to paramilitarism I have drawn largely from those identified by Auten, J. H. (1981). The paramilitary model of police and police professionalism. *Police Studies*, *4*(2), Summer.

Prior to *September 11* some writers had already expressed concern about the shift in policing towards paramilitarism. Weber (1999, p. 2) referring to the USA, for example, expressed alarm at the 'spawning of a culture of paramilitarism in American law enforcement [with] local police officers … increasingly emulating the war-fighting tactics of soldiers.' McCulloch (2001a) also prior to *September 11* considered the threat of terrorism in Australia had been used to justify significant changes in the role of the police and its shift towards paramilitarism. To these writers the civil–military separation was breaking down and the lines that traditionally separated the military mission from the police were becoming distinctly blurred. Moreover, as Weber (1999, p. 5) contends:

> Over the last century police departments have evolved into increasingly centralized, authoritarian, autonomous, and militarized bureaucracies, which have led to their isolation from the citizenry.

If Weber is correct, what she is describing is either a shift from community policing back to the traditional model or that police have not made the transition at all. It should be remembered she made this comment prior to *September 11*. I am concerned that post *September 11* there seems to be a move which would see community policing and all its fine principles undermined by a reversion to the traditional model of policing, rationalized by the need to counter terrorism. McCulloch (2001b, p. 4), referring to Australia, is more cynical as she describes 'community policing [as] the 'velvet glove' covering the 'iron fist' of more military styles of policing.' This is certainly not my observation. While McCulloch and I both accept that paramilitary policing and

community policing are actually complementary (McCulloch, 2001b, p. 4) we do so for different reasons. She considers references by police to community policing are 'rhetoric [and] well published strategies designed to counter the negative image and public antipathy arising from the use of coercive paramilitary tactics.' It is believe that the complement between paramilitary policing and community policing in many countries to mean the maintenance of a capability to counter extreme acts of violence but within a genuine community policing model. As we face the 'war on terror,' rather than moving away from community policing, police commissioners should look to its qualities and specifically note how this policing philosophy can be used to their advantage. To abandon or diminish it would be counterproductive and would undo the conscious drive over the decades which has taken policing to the high level of societal acceptance it now enjoys. It follows, therefore, that I cannot accept comments like those of de Guzman (2002, p. 11) who believes that, '[in] the context of war against terror, some tenets of community policing appear to be inconsistent with the implementation of these new police roles.' He continues, 'The events of *September 11* threaten the utility as well as the continued existence of some community policing ideals on several grounds' (see below). While he concedes community policing should 'probably not be abandoned,' it is appropriate, to examine the four points he suggests support the fact that community policing in its present form would be unable to meet the demands introduced by the threat of terrorism.

First, de Guzman (2002, p. 11) states the philosophical ideal in community policing of winning the hearts and minds of the community will not be effective against terror since one cannot reason with terrorists. It is futile, he continues, for police to try, and patrols should be made aware that they should not deter but detect and prevent violent terrorist acts. I consider this an extremely narrow point of view. Community–police partnerships work best when they are structured to encourage information sharing from all parts of the community. This *especially* includes groups which tend to be unwilling to assist the police. For de Guzman to refer to this fundamental aspect of community policing as 'futile' in the context of prospective terrorism is unproductive. To exclude or isolate any subgroup from a community policing service amounts to more than failing in a civic duty—it also ignores a most important source of information for police to gauge what they are up against (Bayley & Bittner, 1984). Today, a more thoughtful initiative would be to rebuild trust with specific ethnic/cultural communities, through a genuine commitment by police to protect them and their neighbourhoods, workplaces, and places of worship (Lyons, 2002). Community policing when working well will deflect rumours and reduce misinformation and distortion.

Second, de Guzman (2002, p. 11) believes the introduction of strategies against terrorism will negate assumptions of community cooperation and trust that are implicit in community policing. Terrorists are constantly employing deceit, and therefore, he argues, police should be reluctant to invest their trust on such

unidentifiable forces. I take a contrary view. Successful detection and prevention of terrorism depends on information. From experience we know terrorists can successfully occupy a position within a conventional community. A community–police relationship that is based on mutual trust is more likely to uncover matters that are helpful in identifying prospective terrorists. A more formal or authoritarian police–community relationship would distance police from the rest of the community and only reports of actual law breaking are likely to be reported. However, a good community–police relationship would encourage general dialogue and is more likely to uncover valuable suspicious information and this can only be brought about by trust and mutual respect. Enlisting the community in its own defence encourages it to take control of its own destiny.

Third, de Guzman (2002, p. 11) points out that the partnership of community policing where both parties have to reach a consensus about strategies of crime prevention and police operations will fail in today's environment since police will not be able to reveal their strategies to the community. He considers that if in their preparation of counter-terrorism strategies, the police decide to hold back, the community will sense this and consequently trust will be breached and such partnerships will inevitably wither away. Again, I take a distinctly different view on this point. In existing community policing partnerships, the community has never expected that police confide confidential information about investigations or give specific information about operational tactics. So there is nothing essentially different when dealing with terrorism. Further, to take a position that police will decide what is best for the community could be interpreted as arrogant and in breach of a fundamental tenet of public accountability. The community has a right to certain information, and in the context of terrorism, for example, should be made aware of the level of threat so that individuals can make decisions about their own disposition. A basic assumption of community policing is that police are part of the community (as civilians) and that collaboration should exist in how crime, terrorism, and other community problems are addressed. The contribution community policing can make in this area is extremely positive. In terms of prevention it can allow the community to focus on the importance of notifying early warnings/signs, consistent with the spirit that it is in everybody's interest. The community should feel comfortable about coming forward with information no matter how slight they believe its connection to terrorism.

De Guzman's (2002, p. 12) fourth point is that parochial policing is promoted in community policing but the 'war on terror' necessitates broader collaborative policing. The level of collaboration, he contends, should not only be within the department but should include other local departments, federal or state agencies since in the war on terror the planning space may be distant from the target phase. Thus, efforts to make communications and collaborations among and between police departments should be a constant undertaking. In my view, community policing when working effectively is not parochial and in

fact is multidisciplinary on the basis that police by themselves seldom have the answer for all community problems. Community policing, therefore, uses a broad rather than a narrow (parochial) approach. Police regularly work with specialists at a local and national level and in the context of the threat of terrorism they also work at an international level.

Self Assessment Exercise

1. What sis Police Occupational Subculture?

2. Discuss the changing nature of police philosophy since the aftermath of September 11.

4.0 Conclusion

The traditional model of policing relies on paramilitarism characterized by rank-based authority and command and control. In this model, the organizational structure is hierarchical and inflexible making it difficult to meet the challenges of a rapidly changing environment. Policing here is predominantly reactive and unable to develop and sustain close working relationships with the community in controlling crime. Community policing is eminently sensible since it concentrates on crime prevention. The transition to community policing has not been easy for most police services since the prevailing culture of operational police has shown a distinct preference for action orientation and a lack of interest in 'soft' policing with which community policing has been identified. Even for those services which have successfully made the transition it is likely that the tension within the culture still exists and that moves or even suggestions to revert to the traditional paramilitary style would meet with a great deal of support from the rank and file. The world has certainly changed after *September 11* but there is no need to move away from community policing as the prevailing philosophy. Clearly, there has to be a shift of priorities which allows policing strategies to focus on national security. To assume, however, that paramilitarism as an overarching model is best suited to do this is a serious miscalculation. A reversion to a traditional model of policing will undo the decades of great work that has placed modern community policing as an exemplar of public service in a civil and democratic society. Using the principles of community policing is a much more sensible and effective way of dealing with terrorism. It has been accepted that police cannot fight crime alone and must rely on the community. The same principle applies to terrorism. A community– police relationship that is built on trust and mutual respect is much more likely to give early warnings about terrorist acts. Rather than move policing away from community policing it should be reinforced especially in light of the cultural traits in operational police that tend to indicate a preference for action. The commitment of police commissioners over the years to make the necessary transition to achieve this cultural change must not be forgotten. Moreover, as they reconfigure policing

strategies to meet the threat of terrorism (as they must) they should be alert to the likelihood that operational police might prefer to move to an action-oriented style of policing characterized by paramilitarism. In their eagerness to give public reassurance, politicians might prefer this model too. The road ahead will be demanding for police leaders. What must be resisted is the temptation to fall back to the methods of policing which ignore the profound and ethically based principles of community policing.

5.0 Summary

The events of September 11 and the subsequent concern for national security have justifiably shifted the priorities of policing. However, in the so-called 'war on terror' police services might be tempted to abandon (or diminish) community policing and revert to the traditional model of policing with its emphasis on paramilitarism. To do so would not only be counterproductive but would also arrest the progress policing has made over recent decades which has taken it to the high level of societal acceptance it now enjoys. In their haste to give public reassurance, politicians might expect a traditional model and as police commissioners face the challenge of retaining community policing there will be further tension from within the ranks as mainstream police culture is action oriented and likely to prefer a paramilitary approach. Rather than moving away from community policing, police services should look to its qualities and apply its fine principles which ultimately will be more effective than the traditional model. The traditional model of policing will, in fact, distance police from the rest of the community whereas a community policing relationship that is built on trust and mutual respect is much more likely to provide early warnings about terrorists' acts.

6.0 Tutor Marked Assignment

List and discuss De Guzman's four points in support of the existence of community policing in today's terrorised world.

7.0 References/ Further Reading

Auten, J. H. (1981). The paramilitary model of police and police professionalism. *Police Studies, 4*(2), 67–78.

Bayley, D. H. (1994). *Police for the future.* New York: Oxford University Press.

Bayley, D. H., & Bittner, E. (1984). Learning the skills of policing. *Law and Contemporary Problems, 47*(4), 35–39.

Chan, J. (1997). *Changing police culture: Policing in a multi-cultural society.* Cambridge: Cambridge University Press.

D. P. Rosenbaum (Ed.), *The challenge of community policing: Testing the promises.* Thousand Oaks, CA: Sage.

de Guzman, M. C. (2002, September/October). The changing roles and strategies of the police in time of terror. *ACJS Today,* 8–13.

Fitzgerald, G. E. (1989). *Report of a Commission of Inquiry Pursuant to Orders in Council,*
Brisbane Commission of Inquiry into Possible Illegal Activities and Associated Police

Misconduct. Queensland Government Printer.

Lyons, W. (2002). Partnerships, information and public safety; Community policing in a time of terror. *Policing: An International Journal of Police Strategies and Management, 25*(3), 530–542.

McCulloch, J. (2001a). Paramilitary surveillance: S11, Globalisation, terrorists and counter-terrorists. *Current Issues in Criminal Justice, 13*(1), 23–35.

McCulloch, J. (2001b). *Blue army.* Melbourne: Melbourne University Press.
Oliver, W. M., & Bartgis, E. (1988). Community policing: A conceptual framework. *Policing: An International Journal of Police Strategies and Management, 21*(3), 490–509.

Oliver, W. M., & Bartgis, E. (1988). Community policing: A conceptual framework. *Policing: An International Journal of Police Strategies and Management, 21*(3), 490–509.

Prenzler, T. (1997). Is there a police culture? *Australian Journal of Public Administration, 56*(4), 47–65.
Reiner, R. (1992). *The politics of the police* (2nd ed.). Brighton, UK: Harvester.
Roberg, R. R. (1994). Can today's police organizations effectively implement community policing? In
Skolnick, J. H. (1966). *Justice without trial: Law enforcement in democratic society.* New York: John Wiley.

Sparrow, M. K., Moore, M. H., & Kennedy, D. M. (1990). *Beyond 911: A new era for policing.* New York: Basic Books.

Weber, D. C. (1999). Warrior cops: The ominous growth of paramilitarism in American police departments. Retrieved from
www.cato.org/pubs/briefs/bp50.pdf

Williams, E. J. (2003). Structuring in community policing: Institutionalising innovative change. *Police Practice and Research, 4*(2), 119–129.